

Freedom of Information – Response – 27598

This request concerns the council's records management and retention arrangements as they apply to instant messaging applications used for the conduct or discussion of council business, including whether automatic deletion or disappearing message functions are in use on such applications and, if so, how their use is reconciled with the council's records retention obligations.

DEFINITIONS AND SCOPE

In this request:

"messaging apps" means instant messaging applications, including but not limited to Signal, Telegram and WhatsApp;

a "group" means a chat, channel or conversation with three or more participants, created using the group chat function of a messaging app. One-to-one conversations are excluded from the scope of this request except where expressly stated at item 8 below;

references to the council's communications team are to the team or service, however styled, with day-to-day responsibility for the council's media relations, press and public communications;

references to council business are to be read broadly, and include any matter relating to the council's functions, services, decisions, administration, finances or communications, whether or not any formal decision was taken; they are not limited to formal decision-making and do not depend on the forum in which the matter was discussed;

references to "the Leader of the Council" are to Councillor Michael Hadwen throughout the period covered by this request, including the period from 8 May 2026 until his formal election as Leader at the Annual Meeting on 21 May 2026, during which he was leader of the incoming administration; they do not include any previous holder of the office.

Unless otherwise stated, the request covers the period from 8 May 2026 to the date of this request. A group or conversation falls within scope if it existed or was used during that period, whether or not it was created before 8 May 2026; where a group or conversation was created before that date, the creation date requested below may accordingly fall outside the period.

Items 1 to 6 relate to policies, arrangements, advice and instructions in force or applicable at any time during the period, whenever made, issued or configured.

For the avoidance of doubt, items 7 to 9 are intended to be answered by a single enquiry of each relevant individual, and no individual should need to be asked more than once. I anticipate that whether council business has been discussed in a group or conversation can be determined by the participants themselves, without any review of message content

by third parties.

To keep the request proportionate, I am not requesting the content of any messages.

INFORMATION REQUESTED

1. Copies of any policy, protocol, guidance or instruction issued by the council governing the use of messaging apps or other non-corporate communication channels for the conduct or discussion of council business, including any guidance on: the transfer of official information to corporate record systems; the use of auto-delete or disappearing message functions, or of other ephemeral messaging features such as "view once" media or the retrospective deletion of messages for all participants; and the searching of such channels when responding to requests under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004.

[Please see the council's data protection webpage](#) where you can find copies of all the council's information governance policies. All policies apply to staff and councillors (in their role as representative for the council). In particular, the following policy should be of note in relation to managing instant messaging applications – specifically, WhatsApp:

- Staff Acceptable Use of Information and Systems

In addition to the policies, there are two handbooks available on the council's intranet pages. One covers Information Governance for Councillors (first published in 2021 and last reviewed June 2026), and the other is a Records Management Handbook for staff (which is also available to councillors) which was published during June 2026. Both handbooks set out good information governance and records management practices that all staff should follow. Whilst they do not specify exact guidance around the use of instant messaging applications, they have been drafted to give staff and councillors an understanding of council information, regardless of the format in which it is held. Staff and councillors are expected to implement those practices when handling any information, whether in instant messages, emails, word documents, or other.

Both of those handbooks are attached, along with a copy of the council's guidance in relation to using online tools and platforms to collect information which includes when instant messaging apps are suitable for use, when they shouldn't be used, and what's expected in terms of transferring information within instant messages to the appropriate storage solution.

Please note that the policy referred to on page 1 of the online tools and platforms guidance, "Websites, Online Forms and Mobile Applications policy", has not been provided as part of this response because it does not cover instant messaging apps. Instead, it focusses on ensuring that, where services use public facing mobile applications, online forms and webpages, those applications, tools and pages meet the council's obligations around online accessibility.

2. Whether the council's records management policy or retention schedule addresses instant messaging, and if so, the relevant extract.

Appendix C of the Acceptable Use of Information and Systems policy confirms that information contained within WhatsApp messages should be transferred to the relevant case management system and removed from WhatsApp within 24 hours of receipt.

3. The retention arrangements applied to chat and channel messages on the council's corporate messaging and collaboration platform (for example Microsoft Teams), including: the retention period or periods currently configured; whether messages are deleted automatically at the end of any such period or retained indefinitely; when and by whom the current configuration was decided or last changed; and any documented rationale for it.

Teams messages are subject to a default Microsoft retention period and are automatically permanently deleted after 30 days.

4. The retention period or periods that the council considers applicable, under its Records Retention and Disposal Schedule, to each of the following classes of record, including where such records are created on messaging apps: (a) records documenting decisions taken by or on behalf of the council, including Cabinet-level decisions, and the rationale for them; (b) briefings and advice provided by officers to Cabinet Members or other councillors; (c) correspondence and communications between officers and councillors concerning council business; and (d) records relating to the council's media relations and public communications.

Information that evidences council decisions, actions, or business activities becomes a formal record and is kept in line with any relevant statutory or locally determined retention periods, depending on the type of information. Transient communications, draft and duplicate copies, and any information that consists of personal notes, reminders, or working materials, which do not record council business or official activity, are not subject to any retention periods and, in line with good records management practice, should be deleted once they have been actioned or are no longer needed.

In terms of information contained within messaging apps, the above criteria apply, and council policy is that information that needs to be kept should be saved to the appropriate system within 24 hours of receipt. Messages should be deleted once information has been saved. The information that has been transferred to a relevant case management system will be subject to any relevant retention periods, depending on what the information is. Where instant messages are used for transient communication, staff are encouraged to delete them once they have been actioned as a matter of good records management practice.

Records documenting formal decisions and recommendations taken by or on behalf of the Council, including Cabinet, and the reasons for those decisions are recorded in the minutes of the meeting and these will be kept permanently. Agendas and reports presented to support formal decisions taken by the local authority and its committees are also kept permanently. Non-confidential information will be published on the council's website, or (for older documents) are available in paper copy from the Council's public records office for public inspection. Officers should retain any information that is referred to in the background section of reports on the formal agenda, for four years.

Briefings and advice, and correspondence and communications, should be kept in line with any statutory or locally determined retention periods that apply to the type of information that they contain. For briefing papers, if there is no statutory or locally determined retention period, then they should be deleted when they are superseded, or when they cease to apply.

Generally, information relating to the development of film and television, including vlogs and social media, will be kept for three years. Consultation records that relate to links between local people, organisations and decision makers, are kept for six years after

creation. Press releases will remain in the public domain permanently and any records relating to the formation of a press release will be kept in line with the position above.

5. What policies, procedures or technical or organisational safeguards, if any, are in place to prevent auto-delete or disappearing message settings, or other ephemeral messaging features of the kind described at item 1, where used, from destroying information relating to council business before it has been transferred to the council's official record systems.
There is no specific policy, procedure, or technical/organisational safeguard that prevents auto-delete or disappearing messages. Instead, emphasis is placed on staff knowing and understanding what the expectation is around ensuring that council information is saved appropriately so that it can be accessed as required by anyone with a business need, and that records are kept in line with statutory and locally determined retention periods.

In addition, the council has no contract with WhatsApp and is unable to effect any changes on user accounts to ensure that disappearing message functions etc are disabled.

6. Any record of advice, assessment or review by the Data Protection Officer, the Senior Information Risk Owner or the Monitoring Officer concerning the use of messaging apps for the conduct or discussion of council business, including any Data Protection Impact Assessment, together with any instruction, communication or guidance issued to Cabinet Members or officers during the period regarding the retention, deletion or preservation of messages on messaging apps, including any litigation hold or preservation notice.
In addition to the policies and guidance provided above, all of which have been reviewed by the Data Protection Officer during regular corporate policy reviews, please see the attached DPIA that was completed in 2024 in relation to the council's use of WhatsApp. Please note that the guidance that was provided to staff during 2024 now forms Appendix C of the Acceptable Use of Information and Systems policy.

7. Whether any messaging app groups (as defined above, that is, with three or more participants) exist, or have existed during the period, in which council business is or has been discussed, and whose membership comprises:

- a) the chief executive(s) and/or directors, together with one or more councillors;*
- b) three or more Cabinet Members, whether or not officers or other persons are also members;*
- c) the chief executive(s) and/or directors, without any councillor members; or*
- d) one or more members of the council's communications team, at any level of seniority, together with one or more Cabinet Members.*

To keep the cost of compliance manageable, limbs (a) and (c) do not extend to assistant directors or to officers below director level, and references to directors should not be read as including them.

For each such group, please provide: the app used; the group's purpose or name; the categories of member (for example "Cabinet Members", "directors", "communications officers"), rather than the names of individual junior staff; and the date on which the group was created.

Please see the table below.

8. *Whether any one-to-one messaging app conversations exist, or have existed during the period, in which council business is or has been discussed, between the Leader of the Council and either of the Joint Chief Executives. For each such conversation, please provide the app used and the date on which the conversation began.*

Please see the table below.

9. *For each group identified at item 7 and each conversation identified at item 8, whether a disappearing, auto-delete or self-destructing message setting is or has been enabled, and if so: the deletion timeframe applied (for example 8 hours, 24 hours, 7 days, 4 weeks or 90 days); who activated the setting (by role rather than name, where the individual is a junior officer), or whether the setting was applied by default; and the date on which it was activated or changed.*

Please see the table below.

App used	Group's name or purpose	Categories of member	Date of creation	Disappearing message function	Deletion timeframe	Who activated the function	Date function was applied
WhatsApp	Leadership Group	Cabinet members	13 May 2026	Yes	24 hours	Cabinet Member for Planning, Devolution and the Fire Service	Reviewed and updated 3 August 2026
WhatsApp	General	Cabinet members	13 May 2026	Yes	24 hours	Cabinet Member for Planning, Devolution and the Fire Service	Reviewed and updated 3 August 2026
WhatsApp	Announcements	Cabinet members	13 May 2026	Yes	24 hours	Cabinet Member for Planning, Devolution and the Fire Service	Reviewed and updated 3 August 2026
WhatsApp	Cabinet and Deputy members	Cabinet and Deputy members	13 May 2026	Yes	24 hours	Cabinet Member for Planning, Devolution and the Fire Service	Reviewed and updated 3 August 2026
WhatsApp	Cabinet members	Cabinet members	13 May 2026	Yes	24 hours	Cabinet Member for Planning, Devolution and the Fire Service	Reviewed and updated 3 August 2026
WhatsApp	Reform UK SCC Councillors	Councillors, including Cabinet members	17 May 2026	Yes	24 hours	Cabinet Member for Planning, Devolution and the Fire Service	Reviewed and updated 3 August 2026
WhatsApp	Corporate Leadership Team (CLT)	Chief Executives and Directors/Assistant Directors	5 May 2021	Yes	7 days	Not recorded	Not recorded

WhatsApp	One-to-one conversation	CEO (Head of Paid Service) and Leader of the Council	14 May 2026	Yes	24 hours	CEO (Head of Paid Service)	14 May 2026
WhatsApp	One-to-one conversation	CEO (LGR, Devo, Transformation and Change) and Leader of the Council	14 May 2026	No	N/A	N/A	N/A
WhatsApp	One-to-one conversation	Leader of the Council and Assistant Director: Communications and Public Affairs	12 May 2026	Yes	7 days	Leader of the Council	12 May 2026
WhatsApp	One-to-one conversation	Leader of the Council and Communications Manager	21 May 2026	Yes	7 days	Communications Manager	21 May 2026
WhatsApp	One-to-one conversation	Leader of the Council and Communications and Public Affairs Manager	4 June	No	N/A	N/A	N/A

Guidance for Directorates/Services Using on-line tools and platforms to collect information

SCC is increasingly moving towards on-line data collection, consequently it is important to understand what types of data (e.g. non-personal, personal, sensitive data) can be processed via its on-line data collection tools and platforms.

This Guidance sets out the online data collection tools and platforms which can be used for data collection and explains what type (level)¹ of data can and cannot be processed via them.

The guidance also includes data management information for services to ensure that information collected via SCC's on-line tools and platforms is appropriately managed. For more information about records management, see SCC's Records Management Policy [Records Management Policy](#).

For further information about public-facing SCC websites, mobile apps, online forms, including customer portals, online transactional services where people use forms to report issues, make payments, submit requests and applications, see SCC's [Websites, Online Forms and Mobile Applications policy](#).

¹ See SCC's Classification of Information Scheme at Appendix A.

On-line tools and platforms	Suitable for	Not suitable for	Data management
a) SCC website	Publishing public information which includes Green level information only.	Red and Amber level information.	Directorates/services are responsible for regularly reviewing and ensuring that the content of their externally published information is kept up to date.
b) MySCC intranet	Staff information which includes Green and Amber level information which poses little/no risk to privacy (e.g. SCC staff contact details, external generic contact details).	Red level and Amber (e.g. non-generic external contact details) level information.	Directorates/services are responsible for regularly reviewing and ensuring that the content of published information is kept up to date.
c) MS Teams	Short term collaboration, e.g. specific projects, via chat messages, meetings, sharing documents calendar, Tel calls, which may include Red, Amber, and Green level information.	N/A	Data stored in MS Teams is subject to organisational retention policies as outlined in Information Management Policies in Microsoft Teams : Suffolk IT (freshservice.com). This means that MS Teams is not suitable for the storage of client data and case records. All documentation which requires longer term retention should be transferred to the relevant SharePoint site within a service specific agreed timeframe. Services should, prior to any transfers of information to SharePoint, consider data minimisation (e.g. is it necessary

On-line tools and platforms	Suitable for	Not suitable for	Data management
			to keep <u>all</u> of the data for storage purposes?).
d) SharePoint	Primary online storage system for information making it easy to collaborate with both internal and approved external colleagues. Information which includes Red, Amber, and Green level data can be stored on SharePoint.	N/A	Shared drives must not be migrated to MS Teams. Services should, prior to any transfers of information to SharePoint, consider data minimisation (e.g. is it necessary to keep <u>all</u> of the data for storage purposes?). Services should also ensure that SharePoint sites are marked as Private rather than Public where relevant, and that stored documents have appropriate access allocated to them so that only authorised personnel can view them.
e) OneDrive	Personal storage space. OneDrive can be used to store your personal, work-related documents (e.g. PDRs) as well as being used for short term storage of files which may be needed offline or whilst creating documentation which is not ready for publication or wider sharing.	N/A	Once non-personal work related documents are final, they must be moved to SharePoint or MS Teams. Services should, prior to any transfers of information to SharePoint or MS Teams, consider data minimisation (e.g. is it necessary to keep <u>all</u> of the data for storage purposes?).

On-line tools and platforms	Suitable for	Not suitable for	Data management
	You can collaborate with internal colleagues on OneDrive files. Information which includes Red, Amber, and Green level data can be stored on SharePoint.		Services should also ensure that SharePoint sites are marked as Private rather than Public where relevant, and that stored documents have appropriate access allocated to them so that only authorised personnel can view them.
f) Microsoft forms	Creating and sharing surveys, quizzes, and polls. Green and Amber level information which poses little/no risk to privacy (e.g. business email address, partial postcode). If you are already using MS forms for the collection of red or amber level information, please contact your Directorate's SIA for further advice. For example, the service may need to check/update an existing DPIA to ensure its use of MS forms and data management processes are recorded in it. For further advice about using other secure on-line data collection tools, services should contact serviceimprovement@suffolk.gov.uk.	Red and Amber level data which poses a greater risk to privacy (e.g. full name, date of birth, address, contact details, health and care, financial data.).	Information collected via a Microsoft form must be promptly transferred (e.g. within 72 hours of receipt) to the service's permanent storage system and the form containing the information must be securely and permanently deleted.
g) GOSS forms	Customer-facing online forms, which enable payments and transactions	N/A	Directorates/services to work with the Service Improvement team to:

On-line tools and platforms	Suitable for	Not suitable for	Data management
	and manage internal workflow and customer data. Customers are also able to create and manage their accounts. Information which includes Red, Amber, and Green level data can be processed via the Goss platform. Note: there is a significant backlog of requests for GOSS provision which means that requests are managed on a priority basis. Services wishing to use GOSS must ensure they have contacted the Service Improvement team as part of their project planning.		- specify the data that must be collected by the online form - to test the new online service and approve this for going live. A GOSS Request Form must be completed and approved before the new service can 'go live.' The Request Form must specify the data retention period for the information collected via GOSS which will be applied and automatically managed by the system.
h) PowerApps	Creation of bespoke user defined applications to meet niche business requirements not covered by any existing products and services. Requires development and in some cases additional knowledge or skills to operate. Red, Amber, and Green level data can be processed, but Red and Amber level data can only be processed if the system used to store PowerApps generated data is one of the other systems defined in	N/A	This product can integrate to any Microsoft service and also to limited third party services. The system used for storing Power Automate generated data must be one of the systems defined as suitable for storing Red and Amber level data in this Guidance.

On-line tools and platforms	Suitable for	Not suitable for	Data management
	this Guidance as suitable for Red and Amber level data.		
i) Power Automate	Creation of bespoke user defined applications to meet niche business requirements which are not covered by any existing products and services. Requires development and in some cases additional knowledge or skills to operate. Red, Amber, and Green level data can be processed, but Red and Amber level data can only be processed if the system used to store Power Automate generated data is one of the other systems defined in this Guidance as suitable for Red and Amber level data.	N/A	This product can integrate to any Microsoft service and also to limited third party services. The system used for storing Power Automate generated data must be one of the systems defined as suitable for storing Red and Amber level data in this guidance.
j) Mobiles and messaging apps (e.g. WhatsApp, SMS, Facebook Messenger, Viber, Signal)	Instant communications which include Green level and Amber level information which pose little/no risk to privacy (e.g. confirmation of meeting date, time, and location (partial postcode or town only)).	Red level and Amber level information (e.g. information which could pose a risk to privacy such as full name, date of birth, full details of location, reason for meeting).	Customer communications must be promptly transferred to the service's permanent storage system and the information permanently deleted from the mobile/app within, for example 24 hours). See Appendix C in the Acceptable Use policy for guidance in relation to WhatsApp data management.

On-line tools and platforms	Suitable for	Not suitable for	Data management
k) Contensis (Zengenti)	Simple web forms capturing Green and Amber level data (e.g. customer names, email addresses, contact details).	Red level data (any online service requiring sensitive customer data is signposted to an alternative option).	Data collected and stored securely in the Contensis CMS accessed only by platform admins, data also managed by service owners of the forms.

APPENDIX A - SCC's INFORMATION CLASSIFICATION SCHEME

CLASSIFICATION	DESCRIPTION OF INFORMATION TYPES
GREEN	No Impact – Information formally made public by SCC or information which would have no impact on privacy, business, or corporate reputation if it were put into the public domain by any other means.
AMBER	Strictly internal or agreed partners – SCC corporate information which is intended strictly for internal use by staff and agreed partners. Information posing little/no risk to privacy – This could also include customer names, addresses and client numbers that pose little or no risk to privacy.
RED OFFICIAL- SENSITIVE	Health & care personal data – personal data which reveals anything about the health or care arrangements of any individuals or families. This includes details about ethnicity, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation. Financial personal data – personal data which reveals anything about the financial circumstances of any individuals or families Employee & partner personal data – personal data on employees of SCC and its partners. This includes details about ethnicity, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation.
	Impact on health, safety & wellbeing – anything which, if disclosed, would impact on the health, safety, and wellbeing of people. This includes details about ethnicity, gender, or sexuality. Corporate information which would have a significant impact on the reputation or business of SCC if it were seen by non-intended recipient because of commercial, legal, fraud, investigatory or areas where confidentiality is necessary. Special category data as defined under the UK GDPR i.e. personal data revealing racial or ethnic origin ; personal data revealing political opinions ; personal data revealing religious or philosophical beliefs ; personal data revealing trade union membership ; genetic data ; biometric data (where used for identification purposes); data concerning health ; data concerning a person's sex life ; and data concerning a person's sexual orientation . Note: personal data about criminal allegations, proceedings or convictions falls under separate legislation but is classified as red level data.

Data Protection Impact Assessment

You should complete a Data Protection Impact Assessment (DPIA) if you are tasked with assessing the risks relating to the processing of personal data in relation to:

- designing and implementing new technologies
- negotiating new or extending existing contracts which pre-date May 2018
- initiating projects
- reviewing current service provision
- voluntarily sharing information collected by SCC data with external third parties

When the DPIA and its accompanying documentation has been completed, it must be reviewed by the Council's Data Protection Officer & Compliance Manager (DPO). Please send the documents to data.protection@suffolk.gov.uk. **Please note there is a two-week turnaround time (from the date of receipt) for the review of DPIAs.**

Before completing the DPIA, please read the information below.

1. **Before you begin to complete the DPIA, it is recommended** that you map out the dataflows between SCC and the external organisations or contractors. A dataflow diagram should help you to answer the questions in this document. The dataflow diagram should be included as an Appendix to the DPIA.
2. You must answer **all** the questions within the Sections you are completing. To assist with your responses, there are Explanatory Notes throughout the document and two Schedules. Schedule A contains SCC's Information Classification Scheme, which will help you to complete **Section 3**, and Schedule B contains information about the Lawful Bases for Processing Personal Data, which will help you to complete **Section 4**.
3. If you are completing a DPIA for the **purposes of commissioning a contractor who will use personal data under contract**, you must complete **Sections 1, 2, 3, 4 and 5** of this document and a Data Processing Schedule (DPS). **Note:** the DPIA process also applies to situations where a contractor is collecting personal data directly from individuals but is not sharing identifiable data with its commissioners.
4. If you are completing a DPIA for **information sharing** purposes you must complete **Sections 1, 2, 3, 4 and 6** of this document and an Information Sharing Agreement (ISA).
5. If you are completing a DPIA for **Corporate/Directorate/Service development** purposes (e.g., the proposed business developments will mean changing existing data processing purposes to meet new business objectives), you must complete **Sections 1, 2, 3, 4 and 7** of this document (**Note:** if you are commissioning a contractor and/or entering into voluntary external third party information sharing arrangements as a result of the new business objectives you will also need to complete either **section 5 or section 6** of this document).

SECTION 1 – Accountability and Governance

Section 1		Explanatory Notes
1. Project/Contract Name	WhatsApp	
2. Directorate	Corporate Services	
3. Service	Information Governance	
4. Name of Accountable Owner	Stephen Meah-Sims	This is either: the Director, or Asst Director, or Head of Service or Dataset Owner, who is responsible for the data processing risks identified in the DPIA.
5. Job Title	Director of Corporate Services, Deputy Chief Executive and SIRO	
6. Email and phone number	Stephenmeah-sims@suffolk.gov.uk 01473 263512	
7. Name of person completing the DPIA	Anna Stephenson	This is the person to whom the Accountable Owner has delegated responsibility for completing this DPIA.
8. Job Title	DPO + Compliance Manager	
9. Email and phone number	Anna.stephenson@suffolk.gov.uk 01473 264656	
10. State the name of any project/programme board that provides governance for the purposes of this DPIA.	Corporate Leadership Team Corporate Services DMT	If none, record N/A.
11. When will the data processing for the purposes of this DPIA commence?	Retrospective, circa March 2020	An approximate commencement date is acceptable. If the DPIA is retrospective, this should be recorded together with the commencement date of the data processing.
12. How often will this DPIA be reviewed?	Annually	A DPIA is a 'living' document and the service must review it throughout its lifetime.
13. Who is responsible for the DPIA's reviews?	Peter Knight, Head of Information Governance	Either confirm it will be the person completing the DPIA or record the person's name, job title, email, and phone number.
Statement of Accountable Owner:	I confirm I have read and approved the content of this DPIA. E-signature: STEPHEN MEAH-SIMS Date: 6/6/2024	The Accountable Owner must sign this statement prior to the document being sent to the DPO for review.

TO BE COMPLETED BY SCC's DATA PROTECTION OFFICER	
1. DPO's overall assessment RED/AMBER/GREEN	Green
2. Date:	06/06/2024
3. Reasons for DPO's assessment and recommendations	29/01/2026 - DPIA reviewed. Appendix C of the Acceptable Use of Information and Systems Policy has been updated (2025/2026 IG Policies Review) in relation to current usage permissions. 15/08/2024 – Section 7, paragraph 2 updated. 26/07/2024 – Section 7, paragraph 2 updated. 23/07/2024 – WhatsApp clarifications provided at CIGB. 21/03/2024 – Amber
4. Is ICO advice or direction required?	N/A
5. Summarise any ethical considerations in relation to the use of personal data within scope of this DPIA.	N/A
6. Summarise where the DPO's recommendations were not taken or overruled.	22/08/2024 - see Section 7, paragraph 2 updated.
7. In the event of the DPO's recommendations not being accepted, the relevant Director or the SIRO must confirm acceptance of the risks summarised in paragraph (6).	TBC
8. Summary of action(s) agreed by either the Director or SIRO to mitigate/resolve the information risks.	Appendix C of Acceptable Use of Information Systems to be amended to include specific reasons for accessing WhatsApp via BYOD. It is proposed that accountability will be held by the services accepting use of WhatsApp access via BYOD within one or more of the specific reasons.

SECTION 2 – Business context

Section 2		Explanatory Notes
1. Why is this DPIA being undertaken?	Corporate development.	Select the relevant purpose(s) and delete those which do not apply. If your purpose for undertaking the DPIA is not listed, contact the DPO for advice.
2. Summarise the benefits to the public/residents/customers/patients of Suffolk.	a) WhatsApp has become the default method of communication between some of SCC's services and their customers e.g. communications between CYP services and young people and families. b) WhatsApp has become the default of method of communication within services for communicating staff whereabouts (e.g. lone working), absences and meeting arrangements/updates. c) WhatsApp is easy to access e.g. app can be downloaded to mobile phones. d) Messages are instantly communicated to recipients, particularly useful in emergencies arising outside of core hours. e) WhatsApp provides end to end encryption for messages. f) For further context about SCC's use of WhatsApp, see Appendix A.	Whilst DPIAs principally consider compliance risks, they also capture any broader social or economic benefits which the processing of individuals' data for the purpose of this DPIA will bring to the public or communities.
3. What is the greatest risk if a decision was taken to severely limit or totally prevent personal data processing in relation to this project/commissioning?	Services would, in some cases, not be able to effectively communicate with their customers, which could impact on the effective delivery of services. Customers would lose the benefit of a universally	The focus in this section is on the potential for risks – to individuals or to society at large (whether it is physical, material, or non-material) if the processing of personal data for the purpose of

Section 2		Explanatory Notes
	accessible 'free' communications tool. Services using WhatsApp for team communications would lose the 'round the clock' instant messaging benefits of WhatsApp.	this DPIA was curtailed.
4. Will or has this project/commissioning gone through any other formal assurance/governance steps (e.g., Project Gateway Review, formal Board or Committee) before being approved?	YES a) Corporate Services DMT, 30/11/2023. b) Corporate Leadership Team, 13/02/2024 (see paper at Annex A). c) Corporate Information Governance Board, updated on 06/02/2024. d) Core group comments on draft DPIA and appendices reviewed and DPIA updated 22/05/2024. e) IT WhatsApp registration forms reviewed 05/06/2024. f) DPIA sent to SIRO for review and approval 05/06/2024.	If Yes, record the formal assurance/governance steps.
5. Was there any form of public or other consultation (e.g., focus groups, professional body discussion, on-line consultation etc.) in relation to this project/commissioning?	YES SCC - WhatsApp mapping exercise 16/02/2024 to 08/03/2024.	If Yes, record the name(s) and date(s) of the of the consultation(s).

SECTION 3 – Data processing activities and management

Section 3		Explanatory notes
1. List all the AMBER level categories of personal data to be processed for the purposes of this DPIA (e.g., name and address).	SCC employees: mobile nos. Customers: mobile nos. Third parties e.g. partner agencies: mobile nos.	See Schedule A - SCC's Information Classification Scheme.
2. List all the categories of personal data to be processed for the purposes of this DPIA which SCC has classified as RED level data (e.g., financial information).	SCC employees: red level data must not be processed (communicated) via WhatsApp messages. Customers: whilst customers will be told by services not to communicate sensitive information via WhatsApp, there is a possibility that a customer may do so. See Risk Management at Appendix E.	See Schedule A - SCC's Information Classification Scheme.
3. List all the categories of personal data to be processed for the purposes of this DPIA which the UK GDPR defines as special category data (e.g., health, ethnicity).	SCC employees: special category data must not be processed (communicated) via WhatsApp. Customers: whilst customers will be told by services not to communicate special category information via WhatsApp, there is a possibility that a customer may do so. See Risk Management at Appendix E.	See Schedule A - SCC's Information Classification Scheme.
4. List all the categories of NON-PERSONAL data which is sensitive at RED level (e.g., information which is commercially sensitive and/or could have an impact on corporate reputation if disclosed)?	Non-personal emergency information e.g. sensitive location sites could be communicated via WhatsApp.	See Schedule A - SCC's Information Classification Scheme.
5. List all the categories of other NON-PERSONAL (GREEN or AMBER level) data to be processed for the purposes of this DPIA.	Potentially non-personal green or amber level information e.g. meeting location, date, time, could be communicated via WhatsApp.	See Schedule A - SCC's Information Classification Scheme.
6. Does SCC own all the data listed in paragraphs (1) to (5) above?	YES	If No, explain what (if any) data is owned by SCC and list the organisations which own the data together with reason(s) e.g., SCC provides services to organisation A.

Section 3		Explanatory notes
7. List any unique <u>person-related</u> identifiers for the purposes of this DPIA.	Mobile numbers.	For example, NHS number, National Insurance number, social care case-number, IP address.
8. List any other identifiers which are going to be used in relation to assets or property (e.g., Unique Property Reference Number) for the purposes of this DPIA.	N/A	
9. What volumes of personal data (e.g., 100, 10,000, 100,000 people) are likely to be processed for the purposes of this DPIA?	Not known but would estimate >1000 people use WhatsApp for business and operational purposes.	Approximate volumes may be recorded.
10. Will the data processing for the purposes of this DPIA include any information about deceased individuals?	NO – the WhatsApp Data Management Guidance does not permit the inclusion of information about deceased individuals in WhatsApp messages.	If Yes, explain why. Note: DP law applies only to living individuals. Duties of confidentiality will, however, apply to deceased individuals.
11. Is the data processed for the purposes of this DPIA being collected for the first time, or will the processing involve using existing data?	New and existing data	Delete the options which do not apply.
12. If the data processed for the purposes of this DPIA is existing data and is owned by SCC, what is the name of the Dataset's Owner and what is the Dataset's reference number(s)?	SCC maintains records of its data processing activities through each Directorate's Register of Datasets. Information communicated via WhatsApp will be included in the relevant datasets for each Directorate.	This information is available from your Directorate's Register of Datasets (RoDs). The Registers are published on the mySCC DP pages. Your Directorate's SIA will be able to assist with RoDs queries.
13. If SCC is collecting data for the first time for the purposes of this DPIA, what is the name of the Dataset's Owner and what is the Dataset's reference number(s)?	N/A	Ask your Directorate's SIA to add the new dataset to its RoDs and record the Dataset Owner and the dataset's reference number in this section.
14. Do you intend to provide any explanatory materials to data subjects (i.e., customers, patients, clients) about the processing of their data for the purposes of this DPIA?	NO	If Yes, provide details.

Section 3		Explanatory notes
15. Which SCC policies will apply to the processing of data for the purposes of this DPIA?	Acceptable use of Information Systems Data Protection Security Incident Management and Reporting	A list of the policies is available from IT Security Management (sharepoint.com) . List all those which apply.

SECTION 4 – LAWFUL BASES AND INDIVIDUALS’ RIGHTS

Section 4A		Explanatory notes
1. Select one lawful basis for processing data for the purposes of this DPIA. Note: The highlighted options are rarely used by SCC. It is advisable to contact the DPO to discuss your selection of a highlighted option before submitting the DPIA for review.	The lawful basis for processing information communicated via WhatsApp will be included in the relevant dataset(s) within each Directorate’s Register of Datasets.	Select one lawful basis and delete those which do not apply. If SCC owns the data, the lawful basis for processing it should be recorded in your Directorate’s RoDs. If SCC is collecting and processing the information for the first time, see guidance on the mySCC DP pages.
2. Select one additional condition for processing special category data for the purposes of this DPIA. Note: If you are relying on the substantial public interest condition in Article 9(2)(g), you also need to meet one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018. See Schedule B and record the associated condition in this section.	This should not be applicable, however, if for example, a customer were to share special category data via WhatsApp, the lawful basis for processing the information will be included in the relevant dataset(s) within each Directorate’s Register of Datasets.	Select one additional condition and delete those which do not apply. If SCC is collecting and processing the information for the first time, see guidance on the mySCC DP pages.
3. If you are relying on Consent as the lawful basis for processing data for the purposes of this DPIA you must answer the following questions:	N/A	Full answers must be provided in this section. Where appropriate the responsibility for managing consent processes should include job role(s). Details in relation to the management of the withdrawal of consent should include named contact details and the time-frame within which these requests will be actioned.
4. Are you processing any criminal offence data?	Criminal offence data should not be communicated via WhatsApp.	If Yes, complete Section 4B. For definition of criminal offence data see guidance on the mySCC DP pages.
5. Are you processing personal data for law enforcement purposes?	N/A	If Yes, complete Section 4C. Law enforcement purposes are defined as: the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security.

Section 4A		Explanatory notes
6. Which Corporate/Directorate/Service privacy notice applies to the processing of personal data for the purposes of this DPIA?		All SCC privacy notices are published via Privacy and data protection Suffolk County Council .
7. Will the processing of personal data for the purposes of this DPIA require changing the Privacy Notice recorded above?	NO	If Yes, confirm what action has/will be taken to update the relevant Privacy Notice.

Section 4B – Processing criminal offence data	N/A	Explanatory notes
1. Do you have Official Authority to process criminal offence data?		Under Article 10 of the UK GDPR, if your processing is carried out 'under the control of official authority', you do not need to identify a DPA 2018 Schedule 1 condition for your processing, but you must record in this section the legislation/common law underpinning your official authority. If in doubt, contact the DPO.
2. If No, to (1) above you must confirm your lawful basis for processing data remains the same as in Section 4A, paragraph (1) above or record a new lawful basis for processing.		For information about additional conditions see guidance on the mySCC DP pages .
3. You must also confirm your additional condition for processing criminal offence data under Schedule 1 of the DPA 2018.		For information about Schedule 1 conditions see guidance about criminal offence data on the mySCC DP pages .

Section 4C – Processing personal data for law enforcement purposes	N/A	Explanatory notes
8. Are you: a) a competent authority under Schedule 7 of the Data Protection Act 2018 (legislation.gov.uk) or b) do you have statutory functions that give you authority or powers for law enforcement purposes?		If Yes, state whether the service is relying on Schedule 7 or provide details of your statutory authority or powers? If No, the service must not process personal data for law enforcement purposes.

Section 4C – Processing personal data for law enforcement purposes	N/A	Explanatory notes
9. List what categories of personal data are being processed for law enforcement purposes.		
10. Record the legislation underpinning the processing of data for law enforcement purposes.		If the legislation cannot be identified, contact the DPO.
11. Confirm which of these conditions apply to the processing of personal data for law enforcement purposes.		
12. Is any sensitive personal data being processed for law enforcement purposes?		Sensitive processing is defined as the processing of any of the following: · Personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership · Genetic or biometric data used for identification purposes · Personal data concerning health · Personal data concerning an individual's sex life or sexual orientation.
13. Are you relying on consent to process sensitive data for law enforcement purposes?		
14. Is the processing strictly necessary?		Strictly necessary means that the processing has to relate to a pressing social need that cannot be achieved through less intrusive means.
15. Confirm which DPA 2018, Schedule 8 condition(s) you are relying on.		A list of Schedule 8 conditions is available on the mySCC DP pages about law enforcement purposes .

SECTION 5 – CONTRACTORS - ORGANISATIONAL & TECHNICAL COMPLIANCE

PLEASE READ THESE NOTES BEFORE COMPLETING SECTIONs 5(a), (b) and (c)

NOT APPLICABLE

SECTION 6 – INFORMATION SHARING - ORGANISATIONAL & TECHNICAL ASSURANCE

NOT APPLICABLE

SECTION 7 – CORPORATE/DIRECTORATE/SERVICE DEVELOPMENT - Changing existing or implementing new data processing activities to meet new business purposes

Section 7	
1. Briefly explain what is changing and the new business purposes.	a) As per SCC's Acceptable Use Policy, the use of WhatsApp is currently prohibited. b) On 13/02/2024 CLT endorsed the principle that WhatsApp will be able to be used for specified SCC business purposes. This endorsement is conditional upon the following actions which will be required to facilitate its appropriate and safe use by the workforce: i. Undertaking a corporate WhatsApp mapping exercise. The exercise took place between 16/02/2024 and 08/03/2024. The results of the exercise have informed this risk assessment, guidance and communications. ii. Completion of a DPIA. iii. Updating the Acceptable Use policy. iv. Publication of WhatsApp Data Management Procedures. v. Internal communications to workforce to advise of policy change and WhatsApp Data Management Procedures.
2. Having completed Sections 2, 3 and 4 of this document, have you reviewed and updated your data management processes in line with the new business purposes?	YES – see: a) Appendix B – WHATSAPP – Business Purposes and Data Management Procedures. b) Appendix C – draft text for insertion into Acceptable Use and Social Media policies and Councillor Guidance. c) Appendix D – draft text for comms to workforce and Councillors. 26/07/2024 – updates: d) WhatsApp Registration service went live on 01/07/2024. All staff using WhatsApp for business purposes must register. e) InsideSCC comms re WhatsApp on 10/07/2024. f) CIGB updated on 23/07/2024. SFRS have raised issue re WhatsApp registration – meeting to be arranged. g) Accessibility issue in relation to WhatsApp and BYOD raised – meeting to be arranged. h) Core group update on 25/07/2024 (TS): IT have started to put in place the process that will automatically add registration to an active directory group, this group when turned on will then allow only those people in it to install whatsapp, current plan is to add all people who have registered previously to

	the group at the end of August. IT Services will then communicate to all staff that if they have registered by the end of September then IT Services will be uninstalling Whatsapp from their phone Follow up actions: a) SFRS + accessibility issues to be resolved. b) Acceptable use policy to be updated in relation to BYOD not being used to access WhatsApp. c) Email to CIGB reps and SIAs confirming key messages presented at CIGB about use of WhatsApp. 15/08/2024 – updates: a) Meeting on 09/08/2024 to discuss SFRS accessing WhatsApp via personal mobiles (not via BYOD). Attendees: the Head of Information Governance (PK), CYP Product Owner (TS), GHI Product Manager (KT) and DPO (AS). SFRS Group Manager West (PM) who had raised the issue at CIGB was unable to attend. It was agreed that an exception could be made for SFRS users of WhatsApp in this respect. The exception will need to be drafted, agreed and signed off at director level. KT will take this forward with SFRS. b) Acceptable use policy updated in relation to BYOD not being used to access WhatsApp together with explanation updated and published on mySCC DP pages on 13/08/2024. c) Email to CIGB reps and SIAs confirming key messages presented at CIGB about use of WhatsApp sent on 13/08/2024. d) Meeting on 13/08/2024. Attendees: the Head of Information Governance (PK), IT Operations Manager (CS), CYP Product Owner (TS) and DPO (AS). The meeting was advised that the Chief Executive is concerned that WhatsApp cannot be accessed via BYOD. It was agreed that an exemption could be one solution in relation to the Chief Executive's concern. It was also noted that an exemption may have to be applied to Councillors using WhatsApp when conducting council related business. An email response from the Head of Information Governance explaining the outcome of the meeting was sent to the Chief Executive on 13/08/2024. The email includes an explanation about the security risks of an open approach to the workforce accessing WhatsApp via BYOD and the potential for an exemption to be applied for senior leaders.
--	--

	The Chief Executive has advised that she will be discussing the matter further with the SIRO (SMS) on his return to the office. The discussion will include the management of Councillors' access to WhatsApp. Consequently, the draft WhatsApp briefing (31/07/2024) to Councillors is on hold pending the outcome of the Chief Executive's discussion with the SIRO. 22/08/2024 - update: Head of IG (PK) updated CYP Product Owner (TS) and DPO (AS) that following meeting with the SIRO (SMS) the Acceptable Use policy will need to be changed to include accessing WhatsApp via BYOD for specific purposes. The updated policy will also include a list of purposes which it will not be suitable for accessing WhatsApp via BYOD. PK will draft a note in this respect for TS and AS to provide input.
3. Will the new business purposes require you to commission a contractor, or share information with external third parties for the new business purposes?	NO
4. Given the above information what do you consider are the key information/privacy risks in relation to processing data for the new business purposes?	See Appendix E.

SCHEDULE A – SCC's INFORMATION CLASSIFICATION SCHEME

CLASSIFICATION	DESCRIPTION OF INFORMATION TYPES
GREEN	No Impact - Information formally made public by SCC or information which would have no impact on privacy, business, or corporate reputation if it were put into the public domain by any other means.
AMBER	Strictly internal or agreed partners - SCC corporate information which is intended strictly for internal use by staff and agreed partners.
	Information posing little/no risk to privacy - This could also include customer names, addresses and client numbers that pose little or no risk to privacy.
RED OFFICIAL- SENSITIVE	Health & care personal data - personal data which reveals anything about the health or care arrangements of any individuals or families. This includes details about ethnicity, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation.
	Financial personal data - personal data which reveals anything about the financial circumstances of any individuals or families
	Employee & partner personal data - personal data on employees of SCC and its partners. This includes details about ethnicity, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation.
	Impact on health, safety & wellbeing - anything which, if disclosed, would impact on the health, safety, and wellbeing of people. This includes details about ethnicity, gender, or sexuality.
	Corporate information which would have a significant impact on the reputation or business of SCC if it were seen by non-intended recipient because of commercial, legal, fraud, investigatory or areas where confidentiality is necessary.
	Special category data as defined under the UK GDPR i.e. personal data revealing racial or ethnic origin; personal data revealing political opinions; personal data revealing religious or philosophical beliefs; personal data revealing trade union membership; genetic data; biometric data (where used for identification purposes); data concerning health; data concerning a person's sex life; and data concerning a person's sexual orientation. Note: personal data about criminal allegations, proceedings or convictions falls under separate legislation but is classified as red level data.

APPENDIX A

Corporate Leadership Team Meeting

Meeting Date: 13 February 2024

Item	Corporate use of WhatsApp and other messaging tools
CLT Sponsor	Stephen Meah-Sims
Author	Peter Knight – Head of Information Governance Anna Stephenson – DPO and Compliance Manager

1. Purpose of the item

- 1.1 This item is for decision.
- 1.2 The purpose of this item is for CLT to consider the corporate use of WhatsApp and other messaging tools in the light of the risks associated with their use.

2. Links with County Council Priorities and other policy priorities nationally and locally

Looking after our Health and Wellbeing

Suffolk County Council's information governance policies, including its Data Protection Policy, Acceptable Use of Information Systems Policy

Data protection legislation (UK GDPR, Data Protection Act 2018)

3. Key risks, legal or financial implication

- a) If the corporate use of WhatsApp cannot continue, there is a risk that operational teams will not be able to engage efficiently with their client base (especially younger people).
- b) If WhatsApp, and other similar technologies, continue to be used there will need to be a level of IT support to manage the applications.
- c) If WhatsApp, and other similar technologies cannot continue to be used, financial investment would be needed to implement a new messaging technology and provide an IT support service around it.
- d) If the continued use of WhatsApp is approved, there are data protection risks associated with its usage for business purposes (as outlined in this paper).

4. Brief summary of key points

- a) During the Covid-19 pandemic, SCC approved the use of WhatsApp because it was one way of keeping in contact with clients whilst visiting was not permitted. Post pandemic it is not known how widely WhatsApp continues to be used throughout SCC (although it is known that WhatsApp is used extensively by CYP's services).
- b) The reasons why WhatsApp is widely used throughout CYP include:
- i. WhatsApp has become the default method of communication for many young people and families. Email as a communication channel is used far less by younger people.
 - ii. Many young people and their families cannot afford mobile/internet contracts (they usually use a pay-as-you go phone) so WhatsApp has proven to be a key method of making contact, because communication via WhatsApp is free.
 - iii. Operationally, keeping in contact with younger people and families is more efficient when using WhatsApp. Confirmation of appointments has been highlighted as a useful function of WhatsApp.
 - iv. Services have advised that it may be difficult to maintain relationships with some young people if the continued use of WhatsApp is not permitted.
- c) Under SCC's current Acceptable Use of Information Systems policy the use of WhatsApp for business purposes is not permitted¹. This is because WhatsApp is not considered to be secure enough (see paragraph iii below) for the transfer of personal and sensitive data and there is no corporate information governance or IT services guidance in place for managing messaging tools such as WhatsApp. The current information governance risks of using WhatsApp for business purposes include:
- i. Records management: in many instances, SCC has records management systems which keep a central record of people's interactions with services. It is currently not known whether information shared using WhatsApp is routinely transferred to case records, with the risk that the case record may not be as accurate as it should be. Inaccurate information, for example, contact details could potentially cause a data breach.
 - ii. Non-compliance with requestors' rights under information governance law (i.e. Data Protection and Freedom of Information law and the Environmental Information Regulations). Under information governance law the Council has a duty to respond to requestors' requests for

¹ Paragraph 10(b)(i) It is permissible to use SCC's Microsoft Teams messaging tools for sharing any kind of information including RED/OFFICIAL SENSITIVE, either via the written Chat and Post tools or via the video and audio calls function. Paragraph 10(b)(iii) No other form of instant messaging / video conferencing tool should be used for SCC business.

information. Responses will include communications sent via messaging tools, and in the absence of corporate policy and guidance, there is a risk that data collected via messaging tools will be 'missed' which will impact on the Council's ability to fully respond to requests (and thereby not fulfil its obligations under the law).

- iii. Technical security: unlike Microsoft, SCC's IT service does not have a contract with Meta (the owners of WhatsApp). This means that SCC will not have any influence on any technical and security changes made to WhatsApp, or have sight of any technical roadmaps (as an extreme but unlikely example, Meta could choose to remove all encryption from WhatsApp, leaving SCC having to search for alternative messaging technologies)
- d) In August 2023, the Information Commissioner's Office (ICO), (the UK's independent body set up to uphold information rights), issued an official reprimand to NHS Lanarkshire regarding the use of the WhatsApp messaging tool by NHS personnel². The ICO's recommendations for future use of new apps included:

- i. *'Before deploying new apps, consider the risks relating to personal data and include the requirement to assess and mitigate these risks in any approval process.'*

SCC's Data Protection Impact Assessment (DPIA) procedure for assessing and managing information risks is well established. All DPIAs are reviewed by SCC's Data Protection Officer (DPO).

- ii. *'Ensure explicit communications, instructions or guidance are issued to employees on their data protection responsibilities when new apps are deployed.'*

Instructions/guidance in relation to new apps/IT products are published via corporate communications e.g. weekly IT bulletin, Inside SCC.

- iii. *'Review all organisational policies and procedures relevant to the deployment of apps and amend where appropriate.'*

SCC's Information Governance and IT policies are formally reviewed every two years or sooner if required. The review process is managed by a core group comprising representatives from the Information Governance and IT services.

- iv. *'Ensure all staff are aware of their responsibilities to report personal data breaches internally without delay to the relevant team.'*

² [ICO reprimands NHS Lanarkshire for sharing patient data via WhatsApp](#) – ICO website

All personal data breaches are reported via IT Self Service and assessed and managed by the Information Governance team.

5. Timeline Options to Consider

Whilst there is no specific deadline for the decision around the use of WhatsApp, the current position (i.e. not permitted under current SCC policies yet use is continuing), leaves the Council vulnerable to potential risks associated with data breaches or non-compliance with data protection law.

6. Other options to consider

Option 1

Recommend that WhatsApp can continue to be used by SCC's workforce subject to:

- a) Undertaking a Data Protection Impact Assessment (DPIA) to consider the risks relating to processing personal data through WhatsApp, which will include a technical security evaluation. The evaluation will also assess how WhatsApp can be incorporated within SCC's existing technical security processes and systems with a medium to long term view to work with third party suppliers to integrate WhatsApp into their products.
- b) Business analysts undertaking a mapping exercise to determine which services are using WhatsApp and their reasons for doing so. The results of the exercise will be included in the DPIA and will feed into the technical security evaluation.
- c) Providing explicit communications, instructions to the workforce and Councillors on their data protection responsibilities when WhatsApp is used/new apps are deployed. For example, Directorates will need to understand that messages sent and received via WhatsApp and/or other messaging tools will form part of a customer's record which means processes must be put in place to manage the transfer of messaging data to customers' records.
- d) Reviewing and amending where appropriate all organisational policies, procedures, and mandatory training in relation to using WhatsApp/new messaging apps.
- e) Reminding the workforce about their responsibilities to report data breaches without delay via IT Self Service.

Option 2

Recommend that WhatsApp cannot be used, and that alternative messaging methods should be explored and implemented to replace WhatsApp for operational staff. This recommendation will have resource implications, in terms of both cost and staff time.

Option 3

Recommend that WhatsApp cannot be used, and that the existing policy is reinforced, i.e., that Teams is the corporate messaging tool. There is a risk with this recommendation that WhatsApp may continue to be used by teams for operational purposes despite the Acceptable Use policy being in place.

7. Actions

- a) A core group (IT Security Manager, IT Product Owner (CYP), Product Manager (Corporate Services), CYP Business & Information Manager, Head of Information Governance, and the DPO) convened by the Director of Corporate Services and SIRO met on 22 September to discuss the use of WhatsApp. It was agreed that this paper would be prepared for discussion at Corporate Services DMT on 29 November 2023.
- b) In a discussion between the Council's DPO and Essex County Council's (ECC) Information Governance Manager (IGM) about WhatsApp, ECC's IGM confirmed that its policies do not permit the use of WhatsApp.
- c) In the interim communications have been sent out to CYP staff asking them to cease using WhatsApp whilst corporate discussions take place to determine the way forward. However, it is likely that there is continuing use of WhatsApp within some CYP services, and potentially within the wider organisation. A number of CYP teams have expressed concern about the detrimental impact on their services (in terms of communication with families), should the use of WhatsApp not be permitted.

8. Recommendations

This paper was presented to the Corporate Services Directorate Management Team on 29 November 2023. DMT supported Option 1 in the Recommendations at paragraph 6 above. It was agreed that this paper should be presented to the Corporate Leadership Team for their decision in this respect.

APPENDIX B

WHATSAPP – BUSINESS PURPOSES AND DATA MANAGEMENT PROCEDURES

(to be included in SCC's Acceptable Use policy, see Appendix C below . Councillor Guidance will also be updated)

A. Introduction

The Corporate Leadership Team has endorsed the use of the instant messaging tool WhatsApp for specific business purposes (see paragraph B below). Services using WhatsApp for business purposes must comply with the procedures set out in paragraph C below.

Failure to comply with these procedures may result in disciplinary action which could further lead to dismissal and, in some cases, criminal proceedings/prosecution.

B. Business purposes

WhatsApp may be used for the following business purposes:

- a) Where services have agreed with their customers that WhatsApp is their **preferred method of communication**.
- b) Inter-service communications e.g. location whereabouts (lone working), event updates.
- c) Communicating with third parties e.g. contractors, partner agencies for operational purposes.

C. Operational and Data Management procedures for WhatsApp communications between:

1. Services and customers

- a) Services must record on the customer's permanent record why they have agreed to use WhatsApp as their preferred method of communication e.g.
 - more accessible (e.g. economically viable) for customers to use
 - introducing workers (via a video recording) to customers to improve the likelihood of ongoing engagement.
 - inclusivity e.g. sending picture messages which customers using Google Translate can read
- b) Where WhatsApp is used for business services it must only be accessed via SCC managed devices and SCC's BYOD solution [BYOD Index of Articles \(Android and iOS\) : Suffolk IT \(freshservice.com\)](#). Personal mobiles must not be used for accessing WhatsApp for business purposes.

c) Staff wishing to use WhatsApp for business purposes must complete the WhatsApp Registration form which is accessed via IT Self Service.

d) Staff using WhatsApp for business purposes are also responsible for de-registering their use of Whatsapp and must do so using the WhatsApp de-registration form which is accessed via IT Self Service. The form provides guidance in relation to deleting Whatsapp accounts and removal of the app from work mobile devices.

e) Sensitive (i.e. red level and/or special category data) information must not be included in communications (this includes information about deceased individuals).

f) Services must tell their customers not to include sensitive information in their communications with the service.

g) Only the minimum amount of information necessary for the purposes of the message must be used e.g.

‘Appointment confirmed on XX/XX/XXXX. For queries or to cancel call XXXXXXXX.’

h) To ensure customers records are accurate and up to date, all WhatsApp communications between services and their customers must, within 24 hours of receipt, be transferred (i.e. copied and pasted or screenshot saved to record) from the mobile device to the customer’s record on the relevant SCC case management system.

i) The service must also ensure that once customers’ communications have been transferred they are, within the same 24 hour period permanently deleted from the App.

j) If the sending of a WhatsApp message has caused a security incident/data breach, the member of staff must immediately (within 24 hours of discovery) report the incident via IT Self Service.

k) Service managers are responsible for ensuring staff comply with the WHATSAPP – Business Purposes and Data Management Procedures. Any queries about the procedures should initially be discussed with the relevant Directorate’s IG/SIA lead.

2. Inter-services

a) Red level information must not be included in WhatsApp communications e.g. reasons why a colleague is absent.

b) Inter-team WhatsApp groups must be inclusive for the business purposes they have been set up for and should not be used in ways which could cause detriment to individuals or potential organisational disrepute.

- c) Where WhatsApp groups have been formed for emergency purposes, services must ensure that only the minimum amount of information necessary for the purposes of the message is used.
 - d) Where services need to retain records of inter-service communications e.g. emergencies, all communications must, within 24 hours of receipt, be transferred from WhatsApp to the the relevant SCC case management system.
 - e) The services must also ensure that once the communications have been transferred they are, within the same 24 hour period permanently deleted from the inter-service WhatsApp group.
 - f) Where services do not need to retain records of inter-service communications, the communications should be permanently deleted within 24 hours of receipt.
 - g) If the sending of a WhatsApp message has caused a security incident/data breach, the member of staff must immediately (within 24 hours of discovery) report the incident via IT Self Service.
 - h) Service managers are responsible for ensuring staff comply with the WHATSAPP – Business Purposes and Data Management Procedures. Any queries about the procedures should initially be discussed with the relevant Directorate's IG/SIA lead.
3. Services and external third parties e.g. contractors, partner agencies for operational purposes
- a) Red level information must not be included in WhatsApp communications e.g. potentially commercially sensitive data.
 - b) WhatsApp groups must be inclusive for the business purposes they have been set up for and should not be used in ways which could cause detriment to individuals or organisations.
 - c) Where WhatsApp groups have been formed for emergency purposes, services must ensure that only the minimum amount of information necessary for the purposes of the message is used.
 - d) Where services need to retain records of inter-service communications e.g. emergencies, all communications must, within 24 hours of receipt, be transferred from WhatsApp to the the relevant SCC case management system.
 - e) The services must also ensure that once the communications have been transferred they are, within the same 24 hour period permanently deleted from the inter-service WhatsApp group.

- f) If the sending of a WhatsApp message has caused a security incident/data breach, the member of staff must immediately (within 24 hours of discovery) report the incident via IT Self Service.
- g) Service managers are responsible for ensuring staff comply with the WHATSAPP – Business Purposes and Data Management Procedures. Any queries about the procedures should initially be discussed with the relevant Directorate's IG/SIA lead.

APPENDIX C

DRAFT HIGHLIGHTED TEXT FOR INSERTION INTO ACCEPTABLE USE POLICY.
COUNCILLOR GUIDANCE WILL ALSO BE UPDATED

TEXT START

a) **Instant messaging, video and photography:**

- i. It is permissible to use SCC's Microsoft Teams messaging tools for sharing any kind of information including RED/OFFICIAL SENSITIVE, either via the written Chat and Post tools or via the video and audio calls function³.
- ii. All communication using these tools should use professional language, and if any notes need to be kept of meetings where one or more SCC staff is using Teams then such notes need to be kept in the usual way (i.e. exactly in the same way as in physical face-to-face meetings).
- iii. **With the exception of WhatsApp (see sub-paragraph iv below),** no other form of instant messaging / video conferencing tool should be used for SCC business. If an external partner with a different video conferencing tool asks for staff in SCC to take part, then it is the responsibility of the SCC participants to check with IT whether this is possible on technical and security grounds and whether it is suitable. SCC staff who are taking part in such external video conferencing sessions should only provide information up to AMBER level. But Teams should be the preference and if a 3rd party wants to use another meeting solution ask if they will accept an SCC Teams request to host the meeting.
- iv. **The Corporate Leadership Team has endorsed the use of the instant messaging tool WhatsApp for specific business purposes. Services using WhatsApp for any of the specific business purposes listed in Appendix C must comply with the data management procedures set out in that Appendix.**
- v. Unless agreed by your Head of Service and risk assessed through the data protection impact assessment process, no personal instant messaging tools (i.e. those linked to personal non-work social media) can be used for SCC business.

No personally-owned portable cameras or smart phones with cameras can be used to hold or send SCC work related photographs unless it is for GREEN level information. If there is a

³ SCC does **NOT** corporately need to keep audio or video transcripts of outputs from Teams for Business meetings/instant messaging sessions, so it is the responsibility of the meeting host to keep official minutes or to record the meeting etc.

business requirement for photography for AMBER or RED level information, then the business unit needs to risk assess and procure suitable equipment and agree how such data can be transmitted and the format in which it can be held in SCC information systems.

APPENDIX D

DRAFT TEXT FOR COMMS TO WORKFORCE – INSIDE SCC

TEXT START

The Corporate Leadership Team has endorsed the use of the instant messaging tool WhatsApp for specific business purposes. From [enter date] if services are using WhatsApp they must comply with the WHATSAPP – Business Purposes and Data Management Procedures set out in SCC's Acceptable Use of Information Systems policy [insert link].

One of the key conditions of use to ensure customers records are accurate and up to date, will be that all WhatsApp communications between services and their customers must, within 24 hours of receipt, be transferred (i.e. copied and pasted or screenshot saved to record) from the mobile device to the customer's record on the relevant SCC case management system. It is the responsibility of Heads of service/service managers to ensure that staff are complying with this requirement.

Service managers are responsible for ensuring staff comply with the WHATSAPP – Business Purposes and Data Management Procedures. Any queries about these procedures should initially be discussed with the relevant Directorate's IG/SIA lead.

TEXT END

APPENDIX E

WHATSAPP - RISK MANAGEMENT

	Description	Mitigation
R01	Has an Information Risk Assessment been undertaken?	Yes – see DPIA Ref IG/0686.
R02	Customers communicating sensitive (Red level) information via WhatsApp.	The risk cannot be wholly mitigated, but in line with the <i>WHATSAPP – Business Purposes and Data Management Procedures</i> , services must tell customers not to communicate sensitive information via WhatsApp.
R03	Inappropriate message content.	The risk is mitigated by: a) Instructions to staff in the <i>WHATSAPP – Business Purposes and Data Management Procedures</i> about the types of data which cannot be included in messages. b) The procedures will be reiterated in the Councillor's Guidance. c) Updated Acceptable Use of Information Systems and Social Media policies. d) Comms to workforce and Councillors.
R04	Retention, transfer and destruction of message content.	The risk is mitigated by: a) Instructions to staff in the <i>WHATSAPP – Business Purposes and Data Management Procedures</i> about the transfer of messages to SCC's case management

		systems and subsequent permanent deletion of messages post transfer.
R05	Security incident/data breach management	The risk is mitigated by: a) Instructions to staff in the <i>WHATSAPP – Business Purposes and Data Management Procedures</i> about reporting incidents/breaches within 24 hours of discovery.

Information Governance for County Councillors

A practical guide to effective information governance for councillors
Corporate Information Governance team

Contents

Introduction	3
Different councillor roles	3
Division councillors	3
County Councillors	4
Member of a political party	4
Types of information	4
Personal data	4
Non personal data	5
Relevant legislation	5
Classifying information	6
Emails	6
Records Management	7
Data protection fee to the Information Commissioner's Office (ICO)	8
Individuals' rights – subject access	8
Individuals' rights – the right to be informed and privacy notices	9
Other individuals' rights	10
Data protection complaints	10
Information security	11
Lawful bases for processing personal data	12
Processing personal data	12
Processing special category data	14
Processing criminal offence data	14
Use of legitimate interests – general and recognised	15
Withdrawal of consent	16
Information security incidents	16
Information sharing	17
Freedom of Information and Environmental Information	18
Retention of information	18
County councillor – SCC information	18
Division councillor – constituency information	19
Outgoing councillors	19
Casework records	19
Closed cases	19
Open cases	20
Special category data	20
Checking email inboxes and cloud storage	20

1. Information Governance for Councillors Handbook | Version 2.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page 1 of 38

Secure destruction.....	20
SCC records.....	21
Advice and assistance	21
Appendix 1 – Key data protection definitions.....	22
Appendix 2 – The data protection principles	24
Appendix 3 – Classification of SCC information.....	0
Appendix 4 – Checklist for division councillors	2
Appendix 5 – Setting retention periods	4
Appendix 6 – Examples of security incidents.....	0
Appendix 7 – How to report an information security incident.....	3
Appendix 8 – Useful information.....	5
Useful contact details.....	5
Suffolk county council resources	5
ICO resources.....	6

Introduction

Information is a valuable asset which allows organisations to make effective decisions about a range of issues. It is important that as a councillor, you understand fully your responsibilities and how to manage information in compliance with information governance legislation. This will also enable you to conduct your business efficiently.

If it is not managed well, then there can be significant consequences, including:

- loss of reputation
- loss of trust
- formal sanctions from the Information Commissioner's Office (ICO), which could include enforcement notices, reprimands, and financial penalties.

Getting it wrong could also constitute a breach of the Councillors' Code of Conduct which may result in action being taken by the Monitoring Officer.

This guidance, whilst focussing on the role of county councillors as representatives of Suffolk County Council (SCC), also provides information to help you manage your responsibilities and information as a division councillor.

A list of definitions of key words used throughout this guidance can be found in [Appendix 1](#).

Different councillor roles

As councillors, you undertake more than one role. Depending on which role you are in, your responsibilities and obligations will differ when it comes to processing personal and special category data and responding to requests for access to information.

Division councillors

As a division councillor, you are an elected representative of your constituency and will use information to carry out casework on behalf of your constituents. This could include supporting a constituent in issuing a complaint, notes and files from surgeries, or petitions and correspondence about local issues.

Division councillors are controllers for the purposes of data protection law. As a controller, you are responsible for ensuring that your personal data handling practices meet the requirements of current data protection law (UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018).

County Councillors

County councillors are representatives of SCC and will sit on the Cabinet and on committees to make decisions about council business. County councillors may also be district/borough councillors, and/or parish/town councillors. Regardless of whether you are county, district, town or parish, your responsibilities as a representative of the relevant authority, will be similar.

SCC will be the controller for the purposes of data protection law, and you, as county councillor, will be responsible for ensuring that the information that you handle on behalf of the council is done so in line with its policies and processes.

Member of a political party

As a member of a political party, it is the party itself that is the controller and councillors will need to ensure that the information that they handle in that respect is dealt with in line with the party's policies and processes.

Whichever of the above roles you are in, it is important to remember that you must keep information relating to each one separate from the other.

Information relating to your constituency casework must be kept separately from SCC information and party information.

Party information must be kept separately from constituency casework and SCC information.

SCC information must be kept separately from constituency casework and Party information.

Types of information

The information that you process as a councillor can generally be split into two types, personal and non-personal.

Personal data

Personal data is information that relates to, and can be used to identify a living individual, for example, name, address, and date of birth.

More sensitive personal data is called special category data, for example, medical and social care records.

Non personal data

Non-personal information is any information that is not personal data and that relates to business or environmental matters, for example, commercial information, environmental assessments, and contracts.

It is important to note that the above definitions refer to information, rather than documents.

Some documents, such as contracts, can include both *personal data* and non-personal information, for example, names of employees and financial business information.

When you process documents, you will need to take appropriate measures depending on the type and sensitivity of the information contained within.

Relevant legislation

Your use of personal and special category data is governed by:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018 and
- The Data (Use and Access) Act 2025

The UK GDPR contains seven key principles which set out the spirit of data protection law. You can see the principles set out in [Appendix 2](#) below. They are key to your compliance with data protection law.

As a division councillor, you have responsibilities relating to how and when you can use personal data. It is up to you to make sure that you know and understand those responsibilities and have appropriate policies and processes in place that enable you to fulfil those legal obligations.

As a county councillor, any personal or special category data that you process is the responsibility of the council. You must make sure that you follow the council's policies and procedures that are in place for dealing with information. The information in this document will help you to do that.

The Freedom of Information Act 2000 (FOI) and the Environmental Information Regulations 2004 (EIR), provide a right of access to non-personal information that might be held by a relevant authority. This includes SCC.

As a division councillor or member of a political party, it is unlikely that the information you hold will be subject to the provisions of either FOI or EIR.

1. Information Governance for Councillors Handbook | Version 2.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page 5 of 38

However, as a county councillor, any information that you hold on behalf of the council will fall within the access provisions of the legislation. Therefore, you must be able to identify it, locate it and extract it when asked, so that it can be considered for disclosure in line with the council's obligations. Please see Part 16 below for more details about the FOI process at SCC.

Classifying information

One of the fundamental principles of data protection law is that personal and special category data are protected using measures that are appropriate to the level of sensitivity. It is important that councillors are able to identify information classifications as this will help to you make the right decisions about how it needs to be looked after.

As division councillor, you will be responsible for classifying the information that you hold in that respect. Whether you decide to develop a formal classification process is up to you.

Under data protection law, special category data is clearly defined and relates to more sensitive personal data that, if mis-handled, has the potential to have significant effects on the individual to whom it relates.

Because SCC also has a large amount of non-personal data that is equally as sensitive, the council's classification and labelling policy covers not only personal data but extends to include all SCC information.

SCC uses a "traffic light" system to easily classify its information. Please see [Appendix 3](#) for a copy of the different classifications, and examples of the information that each one includes.

Ensuring that you apply the correct classification to the information that you are processing means that SCC is able to focus its controls and resources appropriately, in terms of securing its information; for example, information classified as Red will need more robust security measures in place to protect it than information that is classified as either Amber or Green.

Emails

As a county councillor for Suffolk, you will be provided with IT equipment by SCC, and this will include an individual email account. You may use the SCC email account for both your county councillor role and as a division councillor, and it is the contact email address that will be published on the council's website.

You must not use your SCC email account for purely personal matters, for example, to order things online, or to access your personal social media accounts. Never use your SCC email address to subscribe to non-related external mailing lists, or as a user id on websites that are not related to your role as councillor.

1. Information Governance for Councillors Handbook | Version 2.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page 6 of 38

It is important that you keep your user account ID and password secure - do not share it with anyone else and do not allow anyone else to use your SCC IT device.

The council uses OME (Microsoft Office 365 Message Encryption) which will allow you to label any emails that contain Red level information (please see [“Classifying information”](#) above and [Appendix 3](#) below for more details about classifying information) as Official-Sensitive.

Once you have labelled your email as Official-Sensitive, it will be encrypted before it is sent, to make sure that it remains secure and the label “Official-Sensitive” will be added to the subject header of your email.

As an SCC councillor, your email address will be published on the council’s website. This does mean that you are likely to receive spam and/or “phishing” emails.

Spam emails are unsolicited emails with the main aim being advertising, phishing, fraud or spreading malware. Phishing emails are a specific type of spam email in which the sender poses as a legitimate institution to try and lure you into providing them with information, such as banking and credit card details, or user-names and passwords.

If you receive an email into your SCC email account which you believe might be spam or phishing, do not open it and delete the message. Only open an email if you are certain that it is genuine. If you open a spam email or have responded to a phishing email in error, please contact the IT Service Desk so that they can investigate it further. Do not log into your device or access your account on any other device until IT have confirmed that it is safe to do so.

Records Management

Good records management practices are vital to ensuring that information assets are used as efficiently as possible and in line with any statutory obligations, for example data protection law. It will mean that:

- decisions can be made efficiently and with confidence that the information is accurate
- it is easier to locate and provide information in response to requests, for example, SARs and FOI
- information is not kept for longer than necessary (see [Appendix 2](#), principle number 5, in respect of personal data)

As a county councillor, you must follow the council’s policies (please see the link provided in [Appendix 8](#)) and processes when it comes to processing information, including where information should be filed, how it can be used and how long it should be kept for. If you are unsure, please check with Councillor Services for more guidance.

As division councillor, you should ensure that you implement good records management in respect of any information that you collect and process in that role.

The following Do’s and Don’ts apply as equally to the information that you hold as a county councillor and a division councillor:

1. Information Governance for Councillors Handbook | Version 2.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page 7 of 38

Do • Regularly review your records, both electronic and paper • Make sure that information is saved in an appropriate filing system where it can be accessed by anyone who is authorised to access it • Put in place retention periods for the information that you hold and review it at the end of that period and either destroy it, or re-assess the retention period • Keep information that relates to the different councillor roles separate from each other	Don't • Don't use Outlook folders as a filing system – emails should either be filed appropriately or deleted once they have been actioned • Don't keep information forever, just in case it might be useful. If you no longer have a business need for it, and it has reached its retention date, then delete or destroy it • Don't keep duplicates of information – duplicates and drafts can be deleted once they have been finalised
--	---

Data protection fee to the Information Commissioner's Office (ICO)

Since April 2019, it is no longer a requirement for elected representatives (which includes councillors) to pay a controller's data protection fee to the Information Commissioner's Office (previously known as notification or registration).

It is still a requirement for SCC and any political parties, of which you may be a member, to make sure that they pay the appropriate fee. Therefore, any work that you do on behalf of SCC or a political party, if relevant, will be covered by their fee.

Individuals' rights – subject access

Under data protection law, individuals have several rights, the most common of which is known as the right of subject access, or a subject access request (SAR).

The right of subject access allows individuals to request access to all the personal and special category data that is held by a controller and creates an obligation on controllers to respond in full within one month of receipt (28 calendar days).

Once a request has been received and the controller is satisfied of the individual's identity, then the controller must collate all relevant information, check it and redact any information that the individual may not be entitled to (e.g. personal data that relates to someone else). The controller must then provide the individual with their response that includes copies of their personal and special category data, where appropriate.

As a division councillor (and controller), you are responsible for ensuring that you recognise a SAR when you receive one in respect of information that you may hold about your

constituents. You must also have a process in place that enables you to record and respond to such requests.

Please see [Appendix 4](#) for a useful checklist for division councillors, and [Appendix 8](#) for links to guidance from the ICO, including how to process SARs.

In SCC, SARs are co-ordinated and processed by the Information Governance team (IG team). Therefore, if you ever receive a request from an individual in your capacity as county councillor, requesting copies of information that you or SCC hold about them, [please send it to the IG team](#) without delay so that it can be logged and the process started.

If you receive correspondence from an SCC member of staff asking you to check for and provide any information in response to a SAR, then please make sure that you respond within any timescales given.

You will need to check the following, and anywhere else that it may be held, for any relevant information:

- Electronic files and emails
- Calendar and diary entries
- Any paper notes or records

Individuals' rights – the right to be informed and privacy notices

One of the other key rights under data protection law, is that individuals have the right to be informed about the collection and use of their personal data. This is achieved using privacy notices.

SCC has published its corporate privacy notice, along with directorate and service privacy notices on its website. The personal and special category data that you process as county councillor, will be covered by these notices.

As a division councillor (and controller), you need to make sure that you also keep people informed of how you process their personal data. SCC has produced a privacy notice for councillors to use, and it is also published on the council's website. You can find a link to this privacy notice in [Appendix 8](#) below.

It is important that people who contact you are made aware of this privacy notice so in addition, all emails that you send using your SCC email account have an automatic footer added to them that includes a link to the councillor privacy notice.

Other individuals' rights

In addition to the right of access and the right to be informed, there are other individuals' rights under data protection law. They are:

- The right to request that incorrect or incomplete personal data is corrected or completed (the right to rectification)
- The right to request that personal data is erased (also known as the right to be forgotten)
- The right to restrict processing of their personal data (the right to restrict processing)
- The right to obtain and reuse their personal data across different services (the right to data portability)
- The right to object to processing of their personal data (the right to object)
- Rights around automated decision making

In SCC, there are corporate processes in place that enable the council to respond in line with its obligations under the law that is managed by the Information Governance team. As with SARs, the time limit for response is one month (28 calendar days).

If you receive a request from someone who is seeking to exercise one of the above rights, please send it without delay to data.protection@suffolk.gov.uk so that it can be logged and processed.

As a division councillor, you must be able to recognise these requests and have in place processes to record and respond to them.

Please see [Appendix 4](#) for a useful checklist for division councillors, and [Appendix 8](#) for links to guidance from the ICO in relation to individuals' rights.

Data protection complaints

Under the Data (Use and Access) Act 2025, as a division councillor, you are expected to handle personal data lawfully, securely, and transparently.

A key element of this responsibility is ensuring that individuals can raise concerns or complaints about how you have used/are using their personal data.

Any complaints you may receive about how SCC has or is using someone's personal data should be directed to the Information Governance team so that it can be managed in line with SCC's formal Data Protection Complaint process.

However, you could also receive a data protection complaint as a division councillor where a constituent or individual believes their data has been:

- shared without consent or lawful basis
- used for purposes other than originally intended
- retained for too long

- incorrect, outdated, or misleading
- accessed inappropriately
- not kept secure

Complaints may also arise in relation to:

- Casework handling
- Email communications
- Use of personal devices or messaging platforms
- Political or constituency activity

As a division councillor, you should have a complaint process in place. This does not need to be complex, but it must be clear, consistent, and documented.

Individuals must know how to raise a concern. This could include:

- a dedicated email address
- clear signposting via email signatures or webpages

Complaints should be acknowledged promptly, typically within five working days (as a matter of good practice).

You should make sure that you can identify whether the complaint relates to personal data, understand the nature of the complaint and be able to provide an appropriate response within a reasonable amount of time.

You should maintain a simple record of complaints received, actions taken, advice sought, or escalation made, and the outcomes. This will support accountability and demonstrate compliance if challenged.

Information security

Under data protection law, controllers have an obligation to ensure that, when they are processing personal and special category data, they have in place suitable measures to protect it.

As a county councillor, the information that you process on behalf of SCC is subject to its security measures. You must ensure the security of any SCC information that is in your possession at all times. Current measures that are in place include:

- encrypted mobile devices
- unique user account IDs and passwords
- follow-me printing facilities
- blue bins in offices for secure disposal of information
- card access to buildings
- lockable information storage facilities, e.g. filing cabinets, pedestals
- secure emails, including Official-Sensitive marking and the use of TLS

- not taking SCC IT equipment abroad or accessing SCC data and systems from your personal device when abroad – please see [Appendix 8](#) below.

At the end of your term as county councillor, you must ensure that all SCC information in your possession is returned to SCC. [Please see the section entitled “Outgoing councillors” below.](#)

As division councillor, you will need to make sure that when you collect personal data from your constituents, that you can secure it appropriately, whether you are working from council premises or from home. The more sensitive the information, the more care you must take to look after it.

Consider implementing the following measures:

- Lock away paper information when you are not using it
- Do not store information about or provided to you from your constituents on unencrypted devices
- Make sure that you dispose of information securely when you have finished with it, for example, use a cross-cutting shredder
- Don't leave information where it could easily be accessed by someone who is not entitled to access it – this includes family members
- Make sure that when you send sensitive information, either by post or by email, that you take necessary steps to secure it, for example, checking that you have the correct contact details for the recipient, use encrypted emails, or Royal Mail Special delivery
- Remember to lock your computer screen if you leave it, even for short periods, or shut it down when you no longer need it

Lawful bases for processing personal data

As a Councillor, you must ensure that any personal information you process is done lawfully and in accordance with UK data protection legislation (UK GDPR and the Data Protection Act 2018) ([see data protection principle 1 in Appendix 2 below](#)).

This means that **you must identify and record an appropriate lawful basis** before collecting, using, sharing or retaining personal data. The lawful basis you rely on will depend on the nature of the data and the purpose of the processing.

Failure to identify a valid lawful basis means the processing is unlawful.

Processing personal data

In most circumstances, your processing of personal data will rely on one of the following lawful bases:

a) Public task – Article 6(1)(e)

This will be your primary lawful basis.

You can rely on this where processing is necessary for:

1. Information Governance for Councillors Handbook | Version 2.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page **12** of **38**

- performing your role as an elected representative
- carrying out constituency casework
- undertaking duties that are in the public interest
- exercising official functions that have a clear legal basis

b) Consent – Article 6(1)(a)

You may rely on consent where an individual has given you clear permission to use their personal data for a specific purpose.

However:

- consent should only be used in limited circumstances
- consent must be **freely given, informed and capable of withdrawal**
- you must be able to demonstrate that consent was obtained

c) Legitimate interests – Article 6(1)(f)

This may apply where you are acting outside your formal public function, for example:

- Community engagement activities
- Correspondence not covered by council duties
- Following up informal enquiries

You must ensure:

- the processing is necessary
- the individual would reasonably expect it
- the impact on the individual is minimal
- a balancing test has been considered

d) Recognised legitimate interests – Article 6(1)(ea)

This applies in specific legal circumstances, including disclosing personal data to public authorities (e.g. SCC or health bodies), where those organisations require the data to carry out their own public functions.

This basis is limited in scope and should only be used where clearly applicable.

Processing special category data

Special category data (e.g. health information, ethnicity, political opinions) requires both:

- a lawful basis under Article 6, and
- an additional condition under Article 9

You may rely on the following:

a) Explicit consent – Article 9(2)(a)

Where the individual has given explicit consent for a specific purpose

N.B. This carries a high standard and must be clearly evidenced

b) Substantial public interest – Article 9(2)(g)

This will apply in most casework scenarios, supported by the Data Protection Act 2018. Relevant conditions include:

- statutory and government purposes (Schedule 1, Part 2, Section 6)
- safeguarding of children and individuals at risk (Schedule 1, Part 2, Section 18)
- political activities, including casework (Schedule 1, Part 2, Section 22)
- responding to requests made to an elected representative (Schedule 1, Part 2, Section 23)

You must ensure that:

- processing is necessary for the purpose
- appropriate safeguards are in place

Processing criminal offence data

Criminal offence data includes:

- criminal records or history
- allegations (including unproven)
- DBS or police checks
- information about victims or witnesses
- details of criminal penalties

This type of data requires:

- a lawful basis under Article 6, and

1. Information Governance for Councillors Handbook | Version 2.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page **14** of **38**

- a specific condition under Schedule 1 of the Data Protection Act 2018

You may process this data where necessary for casework, including reliance on:

- Statutory and government purposes (Schedule 1, Part 2, Section 6)
- Safeguarding of children and individuals at risk (Schedule 1, Part 2, Section 18)
- Political activities, including casework (Schedule 1, Part 2, Section 22)
- Responding to requests as an elected representative (Schedule 1, Part 2, Section 23)

You must only process this data where:

- it is strictly necessary
- the individual has provided it in the context of seeking assistance
- appropriate confidentiality and safeguards are applied

Use of legitimate interests – general and recognised

The general legitimate interest basis under Article 6(1)(f) allows you to process personal data in ways that individuals would reasonably expect and that have a minimal impact on privacy, or where there is a justified reason for processing personal data.

Examples include:

- responding to enquiries outside your formal remit
- continuing correspondence with constituents
- local engagement activities

Where you rely on legitimate interests, you must ensure that:

- the processing is necessary for a clear purpose
- the individual would reasonably expect their data to be used in this way
- the impact on the individual is proportionate

The recognised legitimate interest basis under Article 6(1)(ea) allows you to disclose personal data to a public authority, for example Suffolk County Council, or to health organisations, where they need it to carry out their public functions. Recognised legitimate interests apply only in limited circumstances defined in law.

You should not rely on legitimate interests if:

- public task would be more appropriate
- the processing could cause undue impact or harm

Withdrawal of consent

When you rely on consent:

- individuals have the right to withdraw consent at any time
- you must stop processing their data once consent is withdrawn (unless another lawful basis applies)

In practice, most councillor processing will rely on public task, rather than consent, which should be used as the exception, rather than the default.

Key takeaways

- Always identify a lawful basis before you begin to process personal data
- Public task will cover most councillor activities
- You will need to identify additional conditions for special category data and criminal offence data
- Only collect and process the minimum amount of information necessary
- Ensure you have appropriate safeguards in place and maintain confidentiality at all times

There is a useful interactive tool on the ICO website that will help you to decide which legal basis applies when you are processing personal data. Please see the link in [Appendix 8](#) below.

Information security incidents

An information security incident is an incident that affects the security of information, either personal or non-personal. A personal data breach is when a security incident affects the confidentiality, integrity or accessibility of personal or special category data and breaches the security requirements under data protection law.

Please see [Appendix 6](#) for examples of security incidents.

SCC has a corporate process in place for dealing with information security incidents. As a county councillor, if you become aware of an incident that affects SCC data, you must make sure that you report it, via IT Self Service, as soon as possible.

Under data protection law, SCC must notify the ICO within 72 hours of being made aware of a breach if it is likely to have a harmful effect on the person that it is about.

Please see [Appendix 7](#) below for a step-by-step guide on how to report an information security incident in accordance with the council's policy.

As a division councillor, you are a controller and are therefore responsible for ensuring the security of the information that you process for your constituency casework. This means that you must be able to recognise information security incidents, and personal data breaches. You must have in place a process whereby individuals can report security incidents to you. That process must include provision for investigating individual incidents and taking steps to rectify them.

You need to notify the ICO about a personal data breach when the effect of that breach results in a risk to the rights and privacy of the person affected.

If that risk is significant, you must also let the individual affected by the breach know, so that they can take protective action if necessary.

Information sharing

There is a misconception that data protection law will prevent personal and special category data from being shared. This is not true; data protection law will facilitate sharing of personal and special category data provided sharing is done in compliance with the law.

As county councillor, if you receive a request to share SCC information, this request should be passed to the relevant manager who has responsibility for the information so that they can decide in line with SCC's information sharing practices. If you are unsure, please contact either Councillor Services or the Information Governance team. Please see [Appendix 8](#) below which includes contact details.

As a division councillor, you are the controller and can make the decision about whether you wish to share personal and/or special category data when requested.

One of the things that you will need to make sure you are clear about is what your legal basis is for sharing the data, for example if you are relying on the lawful basis of consent to share data, you will need to check with the individual whether they consent to you sharing it with a third party.

The ICO has produced guidance entitled, "Data Sharing: A Code of Practice" which will help you to decide whether to share personal or special category data and how to make sure you do it in compliance with data protection law.

Please see [Appendix 4](#) for a checklist of things you will need to consider before you share personal or special category data in your role as division councillor and [Appendix 8](#) for a link to the ICO's Data Sharing code of Practice.

Freedom of Information and Environmental Information

As per Part 4 above, information that you hold as either a member of a political party or as a division councillor will not usually be subject to FOI provisions. However, as a county councillor you may hold information belonging to SCC, which does need to be considered for disclosure under FOI/EIR legislation if a request is received.

Information that you hold as a county councillor will be subject to FOI/EIR if it has been given to you by SCC, or when you are acting on behalf of SCC, or if you have created it as part of your role at SCC. It does not matter if the information is stored on your SCC device or on your personal device/email account.

In the council, FOI/EIR requests are coordinated by the Information Governance team, and the council has a limited time, 20 working days, in which to provide a full response to requestors.

Therefore, if you receive a request for access to non-personal information that the council holds, then [you must forward it to the Information Governance team as soon as possible](#), so that it can be logged.

If you receive correspondence from an SCC member of staff asking you to check for and provide any information in response to an FOI/EIR request, then please make sure that you respond within any timescales given.

You will need to check the following, and anywhere else where it may be held, for any relevant information:

- Electronic files and emails
- Calendar and diary entries
- Any paper notes or records

Retention of information

Keeping information for longer than you need to can cause significant problems when it comes to storage and management, so it is important to make sure that you review the information that you hold regularly.

County councillor – SCC information

As a county councillor, most of the information that you hold on behalf of SCC will be subject to statutory retention periods. This means that legislation requires certain types of records to be kept for a specified period of time. For example, financial and HR records are typically retained for six years, plus the current financial year.

It is good records management practice to return SCC information to the relevant service when you no longer have a business need to retain it. Alternatively, if you hold copies of SCC information, you should securely delete them or, in the case of physical records,

1. Information Governance for Councillors Handbook | Version 2.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page 18 of 38

dispose of them using the blue confidential shredding bins located throughout SCC buildings.

Where you have created new information in your role as a county councillor, you must ensure that it is provided to the appropriate service where it constitutes a record of a decision, action, or business activity carried out on behalf of SCC. This ensures that the information is retained as part of the council's official records and managed in line with its records management policies.

Division councillor – constituency information

In the absence of any statutory retention periods, as division councillor, you will need to make sure that you have set appropriate retention periods in place for the information that you collect and hold, so that you are not keeping volumes of personal data and other information indefinitely.

A retention period should indicate the length of time information should be kept for in relation to its business value, along with a trigger point, which is the point at which the retention period begins.

The key considerations when looking to implement a retention period are:

- Why the information was collected in the first place
- What business need is there to retain the information?
- Are there any follow-up process that need to be considered, for example, is there a complaint or appeal process that could be triggered that needs to be accounted for?

Please see [Appendix 5](#) below which sets out key considerations when deciding on appropriate retention periods for the different types of information that you might hold as division councillor.

Outgoing councillors

When you stop being an elected representative, either because you step down, or because you are not re-elected, you still have obligations in relation to the management of the personal and special category data that you hold because of your position.

Casework records

Closed cases

Any records that you hold in relation to cases that have been closed *and are unlikely to be re-opened*, should be securely destroyed - see below.

Any records that you hold in relation to cases that have been closed *and are likely to be re-opened*, should be considered on a case-by-case basis and in line with the advice below in relation to Open cases.

Open cases

Any records you hold in relation to open cases (or closed cases that are likely to be re-opened) should be considered in line with the expectations of the individuals they concern.

If you are not sure what your constituents' expectations are, you can contact them to ask.

You can offer constituents options such as:

- Securely destroying the records
- Passing the case file to the new elected representative or
- Giving the casefile to the constituent so they can decide whether they want to pass it on

N.B. casework records **must not be automatically passed to your successor** without consent from your constituent.

Special category data

Under data protection law, councillors only have four days after an election if not re-elected to process (including holding) special category data.

Given the short timescales involved, guidance from the Information Commissioner's Office provides that elected representatives should review any records that contain special category data in advance of any elections, so you have time to consider what to do with the records.

Checking email inboxes and cloud storage

Before leaving office, you should make sure that any personal data linked to your casework is removed from all locations where it may have accumulated.

This includes checking personal and council email inboxes (including sent items and downloads), cloud-storage apps, and any files saved on personal devices.

All casework records stored in these places should either be securely destroyed or handled in line with the constituent's chosen option.

Secure destruction

When records need to be disposed of, they must be **securely destroyed** so that the information cannot be reconstructed or retrieved.

This includes shredding paper records using a cross-cutting shredder, or by putting them in the council's blue confidential bins.

You should use secure-deletion methods for digital files.

Secure destruction is required for any closed casework that is unlikely to be reopened and is also one of the options that constituents may choose when deciding how their information should be handled.

SCC records

Any information that you have been provided with in your capacity as committee member for SCC or that you hold on behalf of the council, for example documents, reports, or information shared with you for committee work, should be returned to the relevant service or, if copies of existing SCC information, securely deleted.

At a glance: What outgoing councillors must do

You continue to have obligations for any personal or special category data you hold after leaving office, regardless of whether you step down or are not re-elected.

Closed cases (unlikely to reopen): securely destroy all records.

Closed cases (likely to reopen): treat them in the same way as open cases.

Open cases: consider the expectations of the constituent; if unsure, contact them to ask.

Constituents may choose between:

- secure destruction of their records
- transferring the case file to the new councillor
- receiving the case file themselves to decide what happens next

Casework must never be automatically passed to your successor without the constituent's consent.

Special category data: if not re-elected, you may only process (including holding records) this data for four days after the election; review such records before elections to allow time for decisions.

Advice and assistance

If you would like further advice and guidance about any of the information provided in this document, please contact either Councillor Services, or the Information Governance team.

If you have any concerns relating to IT security, [please contact the IT Service Desk without delay](#).

All contact details can be found in [Appendix 8](#) below.

Appendix 1 – Key data protection definitions

Controller – Under data protection law, the controller is responsible for making decisions about how personal data is processed and for what reasons. The controller is also responsible for making sure that they comply with their obligations under data protection law. Failure to do so could lead to sanctions from the ICO.

Data protection law – Currently the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Data (Use and Access) Act 2025.

Information Commissioner's Office (ICO) – The ICO is the information governance regulator for England and Wales. The ICO has responsibility for upholding individuals' rights and has power to implement sanctions against organisations who are not meeting their obligations under the law.

Information security incident – an incident that affects the security of either personal or non-personal data, which may result in a personal data breach.

Personal data – information that relates to a living person, that may be used to identify that individual. Examples include:

- Name
- Address
- Date of birth
- Contact details – email address, telephone number

Personal data breach – An information security incident that results in a breach of security of personal data that leads to the accidental or unlawful:

- destruction of
- loss of
- alteration of
- unauthorised disclosure of; or
- access to

personal data stored or otherwise transmitted or processed.

Privacy notice – A published notice that explains a controller's use of personal and special category data, including:

- What personal and special category data is processed
- The purpose for processing that data
- The lawful bases that apply to each part of the processing
- How long personal and special category data will be kept for
- Details about how individuals can exercise their rights in relation to the personal and special category data that a controller is processing

Process(ing) – Any use of personal or special category data including, but not limited to:

- Collecting
- Storing
- Manipulating
- Sharing
- Deleting

Special category data – is more sensitive personal data, and is defined in the UK GDPR as being:

- Personal data that reveals racial or ethnic origin
- Personal data that reveals political opinions
- Personal data that reveals religious or philosophical beliefs
- Personal data that reveals trade union membership
- Genetic data
- Biometric data
- Data about health (including social care)
- Data about someone's sex life
- Data about someone's sexual orientation

Subject access request (SAR) – A request made by an individual for access to the personal data that a controller holds about them.

TLS (Transport Layer Security) – TLS builds on the council's use of Microsoft O365 Message Encryption (OME) by setting up a secure "tunnel" between SCC and other organisations who have TLS in place. This means that if you mark an email as Official-Sensitive and there is a TLS connection in place, the email is guaranteed to be sent securely.

Appendix 2 – The data protection principles

The data protection principles can be found in Article 5 of the UK GDPR and they are the “good house-keeping” rules of data protection law. As long as you can show that when you process personal or special category data, you are within the limits of the principles, then generally, you will be compliant with the law.

They will apply to division councillors, i.e. when you are processing personal data as part of your constituency case work. This is because as a division councillor, you are a controller and are responsible for the personal data that you use in your constituency casework.

The principles are as follows:

1. When you process personal data, you do so lawfully, fairly and transparently (lawfulness, fairness and transparency principle)
2. When you collect personal data, it will be for a specific, explicit and legitimate purpose (purpose limitation principle)
3. When you use personal data, you will collect and use the minimum amount needed to achieve your purpose (data minimisation principle)
4. When you process personal data, you will make sure that it is kept accurate and up-to-date (accuracy principle)
5. You must not keep personal data for longer than you need it (storage limitation principle)
6. You must make sure that you have appropriate security measures in place to protect the personal data that you hold (security principle)
7. You must take responsibility for the ways in which you use personal data and how you comply with the other principles (accountability principle)

Appendix 3 – Classification of SCC information

The purpose of this guidance is to classify all written, spoken and technological information by its sensitivity so that you can decide the appropriate measures you need to take to protect it.

SCC uses a traffic light rating system (i.e. Red, Amber, Green) to identify the sensitivity of its information. Please see the table below for information to help you classify the data you are working with:

SCC classification levels	Definition	Examples of information
RED	Information which poses high risk to privacy. This could include: information about an individual's ethnicity • political opinions • religious or philosophical beliefs • trade union membership • genetic data • biometric data where it is used to identify people • sex life and sexual orientation • gender reassignment • criminal offence data • health information	• Health & Social Care records • Financial information • Employee data • Health, safety and wellbeing • Corporate information e.g. information which would have a significant impact on the reputation or business of SCC
AMBER	Information which poses little or no risk to an individual's privacy. N.B. It should be noted that if the information is contained within a RED level document, or if you are using large volumes of AMBER level data, it should be treated as RED level data – see above	• Business contact information including email addresses, postal addresses and phone numbers • Customer names and addresses • Unique identifiers such as NHS numbers, NI numbers, case management system ID numbers, e.g. Liquid Logic

GREEN	Information which poses no risk to privacy	• Information that would be disclosed under a Freedom of Information (FOI) or Environmental Information (EIR) request • Information that is routinely published, e.g. staff salaries, statements of accounts, Cabinet meeting minutes
--------------	--	--

Appendix 4 – Checklist for division councillors

As a division councillor, you are a controller for the purposes of data protection law. You may use the checklist below as a guide, but you must make sure that as controller, you fully understand your responsibilities and have the correct processes in place. Please see the ICO resources in [Appendix 8](#) for further guidance about your obligations.

Information security

- ☐ Have in place measures to protect the personal data that you hold, for example, lockable filing systems, and encrypted electronic devices
- ☐ Have in place a process for recording and investigating information security incidents and personal data breaches
- ☐ Know when you need to notify the Information Commissioner's Office of more serious information security incidents
- ☐ Have in place processes for notifying individuals when their information has been involved in an information security incident

Individuals' rights

- ☐ Know where the councillor privacy notice is and ensure it is linked to in all communications (there is an automatic statement included on all email correspondence that is sent from your SCC IT account), and on any blogs or webpages that you control
- ☐ Know how to recognise a subject access request and understand when the right of access applies
- ☐ Recognise the other individuals' rights under data protection law
- ☐ Have a policy in place that sets out how you will record requests exercising individuals' rights, both verbal and written
- ☐ Understand when you should redact information when responding to a subject access request
- ☐ Understand the time limits that govern your response to individuals' rights requests and have a process in place to ensure you can comply with those time limits
- ☐ Have in place sufficient processes to allow you to locate and retrieve information so that you can respond to individuals' rights requests

- ☐ Ensure that you can deliver information to an individual securely when responding to an individual's rights request

Information sharing

- ☐ When you receive a request to share information, consider the following:
 - What is the request for sharing trying to achieve?
 - Is there a safeguarding reason for sharing the information?
 - Are there any risks to individuals that may arise as a result of sharing or not sharing?
 - Would the individual think that sharing their information in this way was fair?
 - Could you achieve the same purpose without sharing information?
- ☐ Make sure that if you decide to share any information, you only share the minimum amount required to achieve the purpose
- ☐ Check to make sure you have a lawful basis to share the information (see [the section on lawful bases](#) above, and the link to the ICO interactive tool to establish legal bases in [Appendix 8](#))
- ☐ If you decide to share information, make sure that you apply appropriate security when you send it
- ☐ Make sure that you record your decision, and the reasons for that decision. This includes occasions when you decide not to share information

General good practice

- ☐ When you go on to share constituent information to assist with an issue, make sure that you only send the minimum amount of information necessary and, if you are unsure about who to send it to, consider phoning to check the correct person before you send any information
- ☐ Use your SCC email account as far as possible to ensure that your emails have adequate technical security
- ☐ If you receive personal or special category data in error, do not compound a potential personal data breach by forwarding it on. Instead, contact Councillor Services or Information Governance for advice
- ☐ If a matter involves safeguarding or health/safety concerns, you have a duty to send information to the relevant service within SCC regardless of whether your constituent has given consent for you to do so
- ☐ If you are relying on consent to process personal data, make sure that when you ask for consent, the individual knows exactly what they are consenting to including when information may be shared

Appendix 5 – Setting retention periods

Below you will find a step-by-step approach to setting retention periods for the information you might collect.

Step 1: Identify the type of information.

Start by clearly identifying what the information is and why it exists. Ask yourself:

- Is this a record or a non-record?
- Does it evidence a decision, action, service delivery, or legal obligation?
- Is it personal data, special category data, or non-personal information?
- Is it linked to a specific case, project, individual, or business function?

If the information does not provide evidence of council business, it may not need a formal retention period.

Step 2: Check for existing retention requirements

Before setting a new retention period, you must check whether one already applies:

- **Statutory retention periods** - some records must be kept for a specific time under law (e.g. finance, employment, safeguarding)
- **Corporate retention periods** - may already exist so you should check SCC's Register of Datasets

If a statutory period exists, it must be followed.

Step 3: Consider key retention factors

If no existing retention period applies, consider the following factors together:

- **Business need** - how long is the information needed to deliver or evidence the service? Is it required for ongoing reference, audit, or operational continuity?
- **Legal and regulatory risk** - could the information be needed for complaints, appeals, inspections, or legal challenge? Is there a realistic limitation period that applies?
- **Data protection principles** - is the information personal data? Would keeping it longer than necessary increase privacy risk?
- **Frequency of use** - is the information actively used, occasionally referenced, or rarely accessed?

- **Historical or long-term value** - does the information record significant decisions, policies, or impacts? Could it reasonably be of archival value?

Retention periods should always be justifiable and proportionate.

Step 4: Set a clear retention rule

Once the retention period is agreed, it must be:

- clearly defined (e.g. “6 years after case closure”)
- applied consistently
- supported by a clear trigger event (e.g. closure, supersession, end of contract)

Step 5: Review and disposal

At the end of the retention period, records must be formally reviewed to decide whether they should be:

- securely destroyed
- retained for a further defined period (with justification)
- transferred to Suffolk Archives

Records, and especially personal and special category data, must not be kept indefinitely “just in case”.

Please see the table below which contains examples of recommended retention periods for different information types.

N.B. These examples are illustrative, not exhaustive. Services must always check for statutory or corporate retention periods first.

Retention periods should be:

- clearly defined
- consistently applied, and
- supported by a trigger event (e.g. closure, supersession, contract end)

Summary table – example retention approaches by information type

Information type	Typical examples	Key considerations	Typical retention approach
Policy and governance records	Approved policies, strategy papers, decision and approval records	Evidence decision-making and accountability; may have long-term reference value	Retain while current plus a defined period after withdrawal ; consider archival value for final versions
Project and programme records	Project plans, risk logs, reports, closure documentation	Audit and assurance requirements; potential post-implementation review	Retain for a defined period after project closure ; key records often longer than working drafts
Case files and service delivery records (personal data)	Case notes, assessments, correspondence, decisions about individuals	High legal and privacy risk; often subject to statutory guidance	Retain in line with statutory or LG Inform+ guidance; retention usually triggered by case closure
Routine administrative records	Routine emails, non-decision meeting notes, working trackers	Limited long-term value; duplication common	Short retention period; dispose once superseded or no longer needed
Financial and contractual records	Contracts, invoices, payment records, procurement documents	Statutory and audit requirements; risk of challenge	Retain for defined statutory or guideline period, typically starting after contract end or financial year close
Training and competence records	Training attendance, certificates, assessments	Evidence of compliance and competence; employment considerations	Retain while relevant plus a defined period ; informal learning records usually shorter retention

Appendix 6 – Examples of security incidents

The examples below are all based on real information security incidents that have been reported to SCC via its information security incident process.

Example 1

Scenario:

You are going to Australia for a three-week holiday to visit relatives who live there. You have quite a lot of constituency casework at the moment and know that when you get back, you will be attending a committee meeting at SCC to decide how much budget will be allocated to a new climate change initiative. You take your SCC laptop and mobile phone with you so you can keep in touch with colleagues at SCC and also respond to some constituency enquiries to keep on top of some urgent casework.

Why is this an incident?

There is a small number of countries that you can take SCC IT equipment to (or use your own personal device to access SCC data and systems) outside of the UK, and you can find more information about these countries in the councillor induction pack that was provided by Councillor Services, or by accessing the link in [Appendix 8](#) below for full guidance from IT. These countries are permitted because they meet a minimum standard of data protection.

Any country not on that list does not meet the required minimum standard of data protection and in some instances, for example Australia, they have additional legislation in place that makes it a criminal offence to bring encrypted devices over their borders. Taking SCC devices into Australia will leave you open to criminal charges for bringing encrypted devices over the borders. It will also expose SCC systems and information to forced access by Australian authorities. Because you were lucky and were not arrested at point of entry, no information has been compromised and therefore, this is an information security incident, rather than a personal data breach.

What action needs to be taken?

SCC is the controller because it affects SCC information. This incident needs to be reported via IT Self Service so that SCC can take protective action to ensure that its systems and information are secure. If access has been forced, then SCC will need to consider whether or not the ICO needs to be notified and whether or not it needs to contact any individuals whose information may have been affected. In addition, you may be facing criminal sanctions in Australia.

Note:

You can take personal devices when you go abroad, but you cannot access SCC data and services outside of the specified countries. You are not authorised to access SCC data in any country not included in the list. Please see the link in [Appendix 8](#) below for a link to the full guidance from IT, including the list of permitted countries.

Example 2

Scenario:

You run a blog that you publish online which you use to keep your constituents informed about local issues that you think may be of interest, and to engage with your local community. One day, you decide to include some photos of you sitting at your desk, with your laptop open, as part of a “day in the life of a local councillor” article. You have your diary open on the desk next to you, and your emails open on screen.

A week after you have published the article and photos online, one of your constituents contacts you because they are worried that an email that they sent you is visible on your laptop screen in the photo that you have published. If they zoom in, they can read their name, their email address and all the information that they have provided to you about a dispute they have with their neighbour, including the effect that the dispute has had on their mental health. They are extremely concerned that if they can read it, then other people will be able to, including their neighbour and that this will further damage the relationship between the two.

Why is this an incident?

Although you didn't intend to inadvertently share this information, in doing so, you have shared someone's personal and special category data with people who weren't entitled to access it, in a way that has the potential to have a significant effect on their privacy. In addition, because the information has been published online you have lost control over it and whilst you can take it down, you have no way of knowing who has seen it, copied it, or forwarded it.

What action needs to be taken?

As division councillor, you are the controller because it affects information that you have collected in your capacity as representative of your constituents. Therefore, you need to record the incident, remove the information from your blog without delay, identify how it happened, take steps to make sure that similar incidents do not occur in the future and apologise to your constituent who has been affected by it.

You will also need to consider whether you need to notify the ICO.

Example 3

Scenario:

You are writing a response to Mr Smedley, a constituent who you have been supporting to access adult social care services.

You have heard back from the service, who have provided information about what is available for Mr Smedley, and what would be appropriate for his level of need. In their email response, they have included a detailed summary of Mr Smedley's specific needs and a description as to how they could meet those needs.

You attach the email from the service to your email and press send. Once it has gone, you realise that you have inadvertently added an extra digit into the email address that you sent it to. You try to recall the message but it doesn't work.

Why is this an incident?

Although it was unintentional, you have shared special category data relating to Mr Smedley's social care requirements to an unknown third party. You have been unable to retrieve the information and have lost control which means that this is a personal data breach. The information is of a sensitive nature and could be used to Mr Smedley's detriment if it has fallen into the wrong hands.

What action needs to be taken?

As division councillor, you are the controller because it has affected information that has been provided to you in your capacity as representative of your constituent. Therefore, you need to record the incident, identify how it happened, take steps to make sure that similar incidents do not occur in the future and apologise to your constituent.

You will also need to consider whether you need to notify the ICO.

Note:

If you become aware of any information security incident that affects information that is the responsibility of SCC, please make sure that you log it via IT Self Service as soon as you become aware of it. Please see [Appendix 7](#) below for a step-by-step guide on how to do this.

Appendix 7 – How to report an information security incident

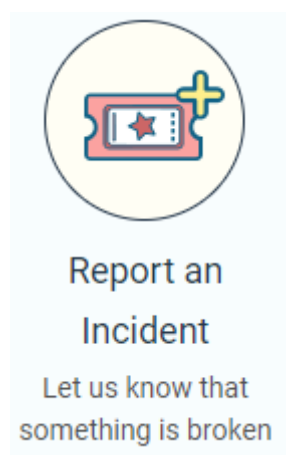
This process is for reporting information security incidents that affect Suffolk County Council information. Incidents must be reported as soon as you become aware that they have happened.

To report a Suffolk County Council incident, follow the steps below:

Step 1 – double click on the IT Self Service icon on your desktop to open the reporting system



Step 2 – click on the “Report an incident” icon on the home screen



Step 3 – complete the form. For the “What do you have a problem with?” section, select “Information security incident” from the top of the drop-down list

What do you have a problem with? *

Details of the issue *

A screenshot of a web form. The 'What do you have a problem with?' section is active, showing a dropdown menu. The menu is open, displaying a list of options: 'Information Security Incident', 'Liquidlogic', 'SystmOne Live', 'Teams and Telephony', 'Mobile Phones', and 'Email'. A blue arrow points to 'Information Security Incident', which is the first option in the list. The dropdown menu has a search bar at the top and a scroll bar on the right.

1. Information Governance for Councillors Handbook | Version 2.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page 3 of 38

Step 4 – in the free text “Describe what has happened” section, please provide information outlining what has happened.

N.B do not provide any personal data here – stick to a summary of the issue

Step 5 – once you have completed the form, including the above, please press submit to log the incident and begin the investigation process

Notes:

1. If you become aware of an incident that has occurred in your capacity as division councillor, you must have in place appropriate processes for recording and investigating incidents. Please see [Appendix 4](#) for a checklist of your responsibilities as division councillor.
2. If you become aware of an incident that has occurred in your capacity as district/borough or parish/town councillor and affects information belonging to that organisation, please contact the relevant council to alert them so that they can investigate as per their local processes.
3. If you become aware of an incident that affects information belonging to a political party and that has occurred in your capacity as a member of a political party, please contact the relevant person within the party to alert them so that they can investigate as per their processes.

Appendix 8 – Useful information

Useful contact details

Councillor Services

Telephone: 01473 265119

Email: councillor.services@suffolk.gov.uk

Information Governance team

Telephone: 01473 265323

Email: data.protection@suffolk.gov.uk or foi@suffolk.gov.uk

IT Service Desk

Telephone: 01473 265999

Email: ITVIPService@suffolk.gov.uk

IT Self Service: <https://suffolk.freshservice.com/support/home>

Information Commissioner's Office

<https://ico.org.uk/global/contact-us/>

Suffolk county council resources

[Information Governance policies](#)

[Councillor privacy notice](#)

[Privacy notice suite](#)

[Suffolk County Councillor intranet](#)

[Guidance around taking SCC devices and accessing SCC information abroad](#)

[Report an information security incident or personal data breach](#)

1. Information Governance for Councillors Handbook | Version 2.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page 5 of 38

ICO resources

[The Information Commissioner's Office \(ICO\) website](#)

[Guide to Data Protection](#)

[Guidance for the use of personal data for political campaigning](#)

[Advice for small and medium organisations](#)

[Lawful basis interactive guidance tool](#)

[Individual Rights – guidance and resources](#)

[Freedom of Information guidance and resources](#)

[Data Sharing: A Code of Practice](#)

Records Management Handbook

A practical guide to effective records management at SCC
Corporate Information Governance team

Suffolk County Council | Endeavour House, Ipswich IP1 2BX

1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page 1 of 63

Contents

Part 1: Introduction to Records Management.....	5
Good records management and SCC corporate goals	5
Compliance with legal obligations.....	6
Why legal compliance matters	6
Legislation and standards	6
Internal standards and policy	7
Part 2: Responsibilities.....	8
Records management for managers	8
Lead and promote good records management practice	8
Ensure records are created, captured, and managed properly.....	8
Maintain compliance with legislation and SCC policy	9
Manage access and information security	9
Oversee storage, retention, and disposal.....	9
Support version control and collaboration	9
Enable business continuity and risk management.....	10
Provide assurance and address issues promptly	10
Records management for staff.....	10
Create and maintain accurate and reliable records	10
Use naming conventions and version control	11
Protect information and apply security requirements.....	11
Comply with legal and policy obligations	11
Store information in the right place.....	11
Manage retention and disposal properly	12
Support business continuity	12
Report issues and seek support when needed.....	12
Dataset owners and managers	12
Dataset owners	13
Dataset managers.....	13
Part 3: Data collection.....	14
Online data collection tools	14
Lawful, fair and transparent	14
Purpose limitation	15
Data minimisation	16
Accuracy	16

1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page 2 of 63

Storage limitation.....	17
Security	17
Accountability	18
Compliance tools associated with data collection and creation	18
Registers of Datasets.....	18
Data Protection Impact Assessments (DPIAs)	19
Privacy notices.....	19
Part 4: Life cycle of records	20
Naming conventions	20
Why use naming conventions?	20
Benefits of using naming conventions	20
Version control.....	20
What is it and why does it matter?	20
Why do we use it?.....	21
Benefits for SCC	21
Draft documents.....	21
Purview labels	22
Reliability of records	22
Duplicates and drafts.....	23
Accessibility.....	23
Storing information	23
Retention	24
Statutory retention periods	25
Corporate retention periods	25
How to set a retention period	25
LG Inform+.....	25
Reviewing records when they reach their retention date	26
Disposal of records	26
Archiving of records	26
Business continuity and back-ups.....	27
Part 5: Management of physical (paper) records	28
Creating physical records and information	28
Storage of physical records	29
Access, movement, and tracking of physical records.....	29
Working away from the office.....	30

1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page 3 of 63

Retention, review, disposal, and archiving of physical records.....	30
Part 6: Security.....	31
Cyber security and awareness	31
How to share and transfer information securely	32
Removable devices (including charging personal devices)	32
Using information away from the office	33
General Principles.....	33
Physical Information.....	33
Electronic Information and Devices	34
Working in Public Places.....	34
Additional Good Practice.....	34
Studying at SCC	34
Third-party access to SCC information and systems	35
Reporting information security incidents and personal data breaches	35
Part 7: Resources.....	36
Policies.....	36
Guidance – including online platforms and tools.....	36
Resources	36
Appendix A – Examples of records and non-records	37
Appendix B – Summary of responsibilities	38
Appendix C – SCC information classification guidance.....	39
Appendix D – Online tools and platforms guidance	41
Appendix E – Naming convention guidance.....	47
Appendix F - How to use version control in SharePoint.....	50
Appendix G – How to check access permissions on Teams.....	53
Appendix H – Where to store records	56
Appendix I – Setting retention periods.....	57
Appendix J – Step-by-step guide to LG Inform+ retention tool	60
Appendix K – Top tips for good records management	62

Part 1: Introduction to Records Management

Good records management and SCC corporate goals

Good records management is essential to supporting Suffolk County Council's (SCC) corporate goals and ensuring that we operate efficiently, transparently, and in compliance with our legal responsibilities.

Effective management of our records and information helps to improve processes and reduce the time needed to carry out essential tasks. It strengthens accountability and audit practices by ensuring that accurate evidence of decisions and activities is maintained across all services.

Records management also plays a crucial role in meeting statutory and regulatory obligations, protecting the legal and other rights of SCC, our staff, and the communities we serve, and preserving information of long-term historical value.

Information and records – what's the difference?

Every day, we create and use large volumes of information, such as emails, notes, spreadsheets, messages, and draft documents.

Information becomes a **record** when it is kept as evidence of a decision, action, or business activity carried out on behalf of SCC. Records provide an official account of what was done, when, why, and by whom. There are some examples of records and non-records in [Appendix A](#).

Not all information needs to be kept as a record, but all information should be handled responsibly. **Good records management practice applies from the point information is created**, not only when something is formally saved or labelled as a record.

All information carries both value and risk. SCC's information is intrinsically valuable because it underpins decision-making daily. By identifying, managing, and mitigating information risks effectively, we protect that value and ensure our information remains accurate, reliable, and fit for purpose.

Risks associated with information, such as non-compliance (which includes retention and review), loss, inaccuracy, or inappropriate access, are managed at a corporate level through tools like the risk register, which feeds into SCC's wider corporate risk management framework.

At service level, information risks are managed by processes including Data Protection Impact Assessments (DPIAs), management of information security incidents and personal data breaches, and the Registers of Datasets (RoDs). By reducing the likelihood and managing the impact of poor records management, we can reduce the overall risk to our information.

1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page 5 of 63

This handbook sets out SCC's approach to creating, using, storing, and disposing of information responsibly throughout its lifecycle, ensuring compliance with legal obligations and supporting efficient and transparent service delivery.

It provides clear guidance on roles and responsibilities, data collection, security, and the management of both digital and physical records.

Compliance with legal obligations

SCC is required to manage its records in accordance with a wide range of legislation, regulatory requirements, and national standards that govern how information is created, used, stored, protected, and disposed of. Good records management ensures we can meet these statutory obligations consistently and demonstrate compliance when required.

Why legal compliance matters

If we fail to comply with legislation relating to records and information, we can expose SCC to significant risks including enforcement action, financial penalties, legal challenge, reputational harm, and disruption to service delivery.

Effective records management helps ensure that:

- information is available, accurate, and reliable
- evidence of decisions and actions is maintained appropriately
- personal and sensitive data is handled lawfully
- records are retained only for as long as they are required and disposed of securely
- requests for information, such as Subject Access Requests (SARs) and Freedom of Information (FOI) or Environmental Information Regulations (EIR) requests, can be met within statutory timescales.

Legislation and standards

SCC's records management practices are shaped by key legislation and standards, including those referenced in this handbook. Core obligations typically include:

- **Data protection legislation** – requiring personal data to be processed lawfully, fairly, transparently, and securely
- **Freedom of Information legislation (including the Code of Practice of the management of records, under section 46)** – requiring public authorities to maintain accessible records so information can be released promptly upon request

- **Environmental Information Regulations** – covering environmental information requests
- **Public Records and Local Government acts** – governing the creation, preservation, and disposal of public records
- **Re-use of Public Sector Information Regulations** – permits the re-use of public sector information for a reason that is different to its original purpose
- **Audit and accountability requirements** – mandating accurate, complete evidence of decision-making
- **Health, social care, education, and safeguarding-related regulations** – requiring specific retention and handling standards for particular types of records

These laws collectively shape how long records must be kept, the controls we must place on access, the security measures required, and the conditions under which information must be disclosed or withheld.

Internal standards and policy

In addition to statutory requirements, SCC must also comply with internal standards and expectations established through its suite of Information Governance and IT policies (which feed into directorate-specific policies and processes).

These policies ensure that organisational practice aligns with legal duties, national standards, and recognised best-practice principles. It provides the foundation for consistent processes across services, ensuring that all staff understand their responsibilities and the legal implications of poor information and records handling.

This guidance should be read alongside SCC information policies, in particular:

- [Records Management Policy](#)
- [Acceptable Use of Information and Systems](#)

Part 2: Responsibilities

Good records management is a shared responsibility at SCC, with managers and staff each playing a vital role in ensuring information is accurate, secure and useable throughout its lifecycle. There is a summary table of the responsibilities below in [Appendix B](#).

Records management for managers

Effective records management relies on managers providing clear leadership, maintaining robust local processes, and ensuring staff understand and fulfil their responsibilities. Managers play a crucial role in creating an environment where information is well-organised, secure, and handled in line with SCC policy, legal obligations, and best-practice standards.

Lead and promote good records management practice

Managers are responsible for setting expectations and modelling good practice in their teams. This includes:

- demonstrating consistent and compliant handling of information in everyday work
- ensuring staff understand the value and risks associated with records, and the impact poor practice can have on service delivery, legal compliance, and audit
- ensuring that records management supports SCC's corporate goals by promoting efficiency, transparency and accountability

Ensure records are created, captured, and managed properly

Managers must make sure their teams:

- create accurate, reliable records of decisions, actions, and business activity
- store and capture records appropriately using agreed systems – Microsoft Teams, SharePoint, OneDrive, and approved line-of-business systems (for example, GOSS, LiquidLogic)
- avoid unnecessary duplication and ensure drafts are managed in line with SCC guidance
- follow naming conventions for documents, records, and folders to support findability, version control and collaboration

Maintain compliance with legislation and SCC policy

Managers are accountable for ensuring their team complies with:

- data protection legislation and associated requirements for lawful, transparent, secure handling of personal and sensitive data
- Freedom of Information, Environmental Information Regulations, and other access-to-information duties
- internal SCC policies and standards that support consistent, compliant information handling

This includes ensuring staff are aware of their obligations, receive and complete appropriate training, and follow local processes.

Manage access and information security

Managers must make sure:

- staff understand and apply SCC's classification guidance (Red/Amber/Green) to protect information appropriately – see [Appendix C](#) for a copy of this guidance
- access to information is restricted to those who need it, and permissions in Teams/SharePoint are checked regularly
- sensitive information is handled, shared, and stored in secure ways consistent with SCC information governance and security requirements

Oversee storage, retention, and disposal

Managers are responsible for ensuring information in their area is:

- stored in the correct location and format (Teams, SharePoint, OneDrive, local systems, or physical storage)
- assigned an accurate retention period in line with statutory and corporate requirements
- reviewed at the end of retention and either securely disposed of or archived if it holds long-term value
- not kept longer than necessary, which avoids unnecessary risk and storage burden

Support version control and collaboration

Managers must promote good version control practices to support efficient and accountable working, ensuring their teams:

- work within SharePoint where versioning is automatically applied

- use version history, compare features, and comments appropriately during collaborative editing
- avoid working offline or saving local copies where version history may be lost

Enable business continuity and risk management

Managers should make sure their area:

- maintains up-to-date information required for operational continuity
- ensures that key records are backed up and recoverable in line with corporate arrangements
- identifies information-related risks and mitigates them using tools such as DPIAs, the Registers of Datasets, and the risk register

Provide assurance and address issues promptly

Managers are responsible for identifying and addressing gaps in records management within their teams by:

- conducting regular checks to ensure compliance
- addressing poor practice proactively
- seeking guidance from Information Governance when needed
- supporting staff during audits, SARs, FOIs and other statutory requests that rely on good records management

Records management for staff

Every member of staff has an important role to play in ensuring that SCC's information is created, used, stored, and disposed of correctly. Good records management supports transparency, accountability, compliance with legal obligations, and effective service delivery across SCC. Staff are expected to handle information responsibly at every stage of its lifecycle.

Create and maintain accurate and reliable records

Staff should:

- create clear, complete, and accurate records of decisions, actions, and business activities
- ensure records are captured in the correct corporate systems (Teams, SharePoint, OneDrive, business applications), rather than stored in personal drives or email inboxes
- avoid keeping unnecessary duplicates and ensure drafts are managed appropriately

Use naming conventions and version control

Staff are expected to use suitable naming conventions for documents, records, and folders to ensure information is easy to find, understand, and manage. Please see [Part 4: Life cycle of records](#) below for more detailed guidance on naming conventions.

Staff must:

- name files in a clear, consistent and descriptive way
- use version control in SharePoint to support collaborative working, avoid confusion, and maintain a full audit trail

Protect information and apply appropriate security measures

All staff must handle information securely and in line with SCC's classification and labelling rules. This includes:

- identifying the appropriate Red/Amber/Green classification to all information (see [Appendix C](#))
- ensuring access is restricted to those who need it and reporting any concerns about inappropriate access
- following SCC's information governance and security requirements when disposing of or sharing information

Comply with legal and policy obligations

Staff must ensure their information handling is compliant with:

- data protection legislation for the lawful and secure use of personal data
- Freedom of Information and Environmental Information Regulations for responding to information requests
- internal SCC policies, procedures, and guidance

This includes responding promptly to SARs, FOIs and internal information requests by ensuring records are accessible and accurate.

Store information in the right place

Staff are responsible for:

- storing records only in approved locations such as Teams, SharePoint, OneDrive, or approved systems
- avoiding the use of local drives or personal areas unless there is a clear business need
- ensuring any physical records are stored securely and appropriately

Manage retention and disposal properly

Staff must follow SCC retention rules and ensure that:

- records are kept only for as long as they are required under statutory, corporate, or locally determined periods
- records reaching the end of their retention period are reviewed and either securely disposed of or archived
- sensitive or confidential records are disposed of using approved secure methods

Support business continuity

Staff must ensure key information required for the continuity of services is stored in shared systems, so it remains accessible if individuals are absent.

Report issues and seek support when needed

All staff have a responsibility to:

- report concerns about incorrect storage, missing information, or poor records management practices
- seek guidance from their manager, Strategic Information Agent, or Information Governance if they are unsure how to handle information correctly
- complete SCC's annual statutory e-learning training, "Our Information, Our Responsibilities", to refresh and maintain their information governance knowledge

Dataset owners and managers

Dataset owner and manager roles can be found in the Registers of Datasets (RoDs). Dataset owners will usually be the Assistant Director or Head of Service of the area using the dataset. Dataset managers will be the operational managers who oversee how the datasets are being used on a daily basis.

Similar datasets may have different owners and managers if they are being used by different services for different reasons.

For more details about the Registers of Dataset, and a description of what a dataset is, please read [Compliance tools associated with data collection](#) under Part 3: Data collection below.

Dataset owners

Dataset owners are accountable for ensuring that a dataset is collected, used, shared, retained and disposed of lawfully and appropriately.

They are responsible for defining the purpose of the dataset, ensuring there is a valid lawful basis where personal data is involved, approving retention periods, and ensuring the dataset is accurately recorded and kept up to date in the Register of Datasets.

Dataset owners provide assurance that risks have been identified and managed, including overseeing DPIAs and privacy notices where required, and act as the escalation point for issues relating to compliance, risk, or appropriate use.

Dataset managers

Dataset managers are responsible for the day-to-day management of a dataset on behalf of the dataset owner.

This includes ensuring data is accurate, complete and up to date, stored securely in approved systems, and handled in line with SCC policies, retention rules and information classification requirements.

Dataset managers ensure that operational practices reflect the agreed purpose and controls of the dataset, keep supporting documentation up to date, and raise issues or changes with the dataset owner where risks, processing activities, or business needs change.

Part 3: Data collection

The UK GDPR sets out seven data protection principles which are essentially the good housekeeping rules of managing personal data. These principles apply whenever SCC collects personal data and should be considered **before, during, and after data collection**. Applying them consistently helps to ensure that personal data is handled lawfully, fairly, securely, and in a way that supports effective service delivery.

While these principles apply specifically to personal data, they also provide a strong foundation for the collection and handling of non-personal information across SCC so the guidance provided in this part should be applied equally to personal and non-personal information, both at point of collection and throughout the lifecycle of the information.

Online data collection tools

SCC is using online systems more often to collect information. These tools include (but are not limited to):

- Microsoft Forms
- GOSS Forms
- SharePoint
- Teams

It is important for staff to understand what kinds of data can be collected using these systems, such as non-personal data, personal data and sensitive data.

Please see [Appendix D](#) for a copy of SCC's online tools and platforms guidance for information about what types of data are allowed on each one. It also explains how information collected online must be managed so it is kept, stored and disposed of properly, in line with SCC's Records Management Policy.

The principles below, and guidance in this handbook apply to all collection methods, both online and offline, as well as manual data collection.

Lawful, fair and transparent

Personal data must be collected lawfully, fairly, and in a transparent manner. This means SCC must have a valid lawful basis for collecting personal data, collect it only for clear and legitimate reasons, and ensure that people understand how their information will be used.

When collecting personal data, staff must:

- be clear about why the data is needed and how it will be used
- only collect data that is relevant to delivering a service or meeting a legal obligation
- provide individuals with appropriate information, usually through a privacy notice, at the point of collection or as soon as reasonably possible

When collecting **non-personal data**, services should still collect the appropriate amount of information needed for the purpose and should be clear and transparent about why the information is being gathered and how it will be used.

Transparency supports trust and helps individuals understand their rights while ensuring SCC can demonstrate compliance.

Being clear about purpose and expectations supports trust with partners, suppliers, and the public, and ensures information is not collected unnecessarily or used in ways that could undermine confidence or accountability.

Purpose limitation

Personal data must be collected for specified, explicit, and legitimate purposes, and not used in a way that is incompatible with those purposes.

Before collecting personal data, services should be clear about:

- the specific purpose the data will be used for
- whether the data may need to be shared internally or externally
- whether the data could reasonably be needed for another lawful purpose in the future

Non-personal data should be collected for clearly defined and legitimate business purposes. Services should be clear about how the information will support service delivery, decision-making, statutory functions, or reporting requirements, and avoid collecting or repurposing information without a genuine business need.

Personal data should not be collected “just in case” or reused for new purposes without considering whether this is lawful and appropriate.

Clear purpose helps prevent misuse and supports consistent records management.

Data minimisation

Under data protection law, the collection of **personal data** must be limited to what is necessary for SCC's legitimate purposes – also known as the principle of data minimisation.

Only information required to deliver services, meet legal obligations, or support business functions should be gathered, and it must be obtained transparently.

When collecting data, staff should:

- consider what information is genuinely required to deliver the service
- avoid collecting additional or excessive detail that is not needed
- periodically review forms, templates, and systems to remove unnecessary data fields

Only **non-personal information** that is necessary and relevant to the intended purpose should be collected. Excessive or overly detailed data can create unnecessary complexity, storage pressures, and management burden.

Data minimisation reduces risk, improves data quality, and ensures information remains focused, useful, and easier to maintain over time.

Accuracy

Personal data should be accurate and, where necessary, kept up to date.

At the point of collection, staff should:

- take reasonable steps to ensure data is correct and complete
- avoid assumptions or informal recording of personal information
- provide opportunities for individuals to confirm or update their details where appropriate

Non-personal data should be accurate, reliable, and appropriate for its intended use, particularly where it supports planning, performance, reporting, or operational decisions. Inaccurate or outdated information can lead to poor decisions, inefficiency, or reputational risk, even where no personal data is involved.

Accurate data supports good decision-making, effective service delivery, and reduces the risk of harm or complaints arising from incorrect information.

Storage limitation

Personal data should not be kept for longer than necessary for the purposes for which it was collected.

When collecting data, services should:

- be aware of applicable retention periods, whether statutory, corporate, or locally determined
- ensure data is recorded in systems that allow it to be reviewed, retained, or disposed of appropriately
- avoid creating duplicate datasets or unmanaged local copies

Non-personal data should not be kept indefinitely without justification. Retention periods should be applied wherever possible, taking into account business need, statutory requirements, historical value, and ongoing usefulness.

Thinking about retention at the point of collection helps ensure data is managed responsibly throughout its lifecycle.

Regular review helps prevent the accumulation of obsolete information and ensures that data continues to add value.

N.B. See the section on [Retention](#) under Part 4: Lifecycle of records below, and [Appendix D](#) for detailed guidance about setting retention periods and what to consider.

Security

Personal data must be collected and handled in a way that ensures appropriate security, including protection against unauthorised access, loss, or damage.

At the data collection stage, staff must:

- use approved systems and secure methods to collect information
- apply SCC information classification (Red, Amber, Green) appropriately (see [Appendix C](#))
- restrict access to those who need the information to perform their role

Although **non-personal data** poses lower privacy risks, it may still be commercially sensitive, operationally critical, or reputationally important. Appropriate security controls should be applied to protect information from loss, unauthorised access, or misuse, in line with SCC classification and security requirements.

Secure collection practices reduce the risk of data breaches and ensure personal information is protected from the outset.

Accountability

When it comes to **personal data**, SCC must be able to demonstrate compliance with each of the data protection principles. In practice, this means that when collecting personal data:

- services must be able to explain why the data is being collected and which lawful basis is being relied upon
- the Registers of Datasets, DPIAs, and privacy notices must be kept up to date
- staff must follow agreed processes, guidance, and training

Accountability ensures that data collection decisions are consistent, justified, and defensible if challenged.

SCC should be able to demonstrate that decisions about the collection and use of **non-personal data** are justified, proportionate, and aligned with business needs.

Clear ownership, documentation of purpose, and consistent application of records management practices support accountability and enable effective information governance across SCC.

Applying the data protection principles to both personal and non-personal data at the point of collection or creation supports good records management, reduces risk, and ensures the integrity of information throughout its lifetime.

Compliance tools associated with data collection and creation

SCC has a number of tools available that should be considered when collecting or creating new information.

Registers of Datasets

A dataset, for the purposes of SCC's Registers of Datasets (RoDs), is a high-level grouping of information that describes a distinct area of processing carried out by a service within SCC.

Datasets represent how a particular set of information is collected, used, shared, retained, and disposed of to support a specific business function or service, rather than individual records or files.

The RoDs are used to meet SCC's obligation to maintain a Record of Processing Activities (ROPA) under UK GDPR and contain datasets which may include personal data, non-personal data, or a combination of both.

If the information you are collecting or creating is a new dataset, then you will need to make sure that it is added to the RoDs if it doesn't exist already.

Data Protection Impact Assessments (DPIAs)

Data Protection Impact Assessments (DPIAs) are required under data protection law when we process personal data. It is extremely unlikely that a DPIA will be required for the processing of purely non-personal data, although not impossible.

However, if you are collecting personal data for the first time, using existing personal data for a new reason, or, if you are reviewing existing personal data collection processes, it is likely that you will need to complete a DPIA (if there isn't one that already covers the processing) to ensure that any risks associated with the processing are captured and mitigated appropriately before collection takes place.

Privacy notices

Privacy notices are a key component of ensuring that SCC is transparent about the way it uses personal and special category data. They ensure people are fully informed about how SCC uses their personal data. They must clearly set out what personal data is being collected, the purposes for which it is used, the lawful basis relied upon, who it may be shared with, and how long it will be retained.

SCC has a full suite of privacy notices that are reviewed on a regular basis. Staff should refer people to SCC's privacy notices when collecting or using personal data to ensure they are clearly informed about what personal data is being collected, how it will be used, who it may be shared with, and the rights available to them. This ensures that people receive accurate, consistent information about their rights and how to exercise them.

Privacy notices must be accessible, easy to understand, and available at the point data is collected or as soon as reasonably possible thereafter.

Part 4: Life cycle of records

Naming conventions

Why use naming conventions?

Although there is no corporately prescribed naming convention within SCC, using a clear and consistent naming convention is an essential part of good records management practice. A well-structured file name helps staff quickly understand what a document or folder contains without needing to open it, making it easier to store, retrieve, and share information appropriately.

Naming conventions typically include elements such as the subject, date, version, and author or team, arranged in a logical and predictable order. This ensures that documents can be identified at a glance and reduces ambiguity when multiple people or teams work together.

Benefits of using naming conventions

Consistent naming of files and records improves efficiency by making information easier to locate, reducing time spent searching for documents and minimising duplication. It also supports accountability and audit processes by ensuring records are clearly identified and reliably traceable throughout their lifecycle.

Good naming conventions reduce the risk of errors—such as working on the wrong version of a document—by helping staff distinguish between drafts, duplicates and final versions. Ultimately, adopting clear naming practices strengthens overall records management and contributes to compliant, organised and transparent information handling across the organisation.

See [Appendix E](#) below for guidance and a suggested naming convention format.

Version control

What is it and why does it matter?

Version control keeps track of every change to a file so we can collaborate safely, work efficiently, and always recover previous versions if needed. SharePoint has version control built in — you don't need to install anything. Every time you edit a file in a SharePoint document library, SharePoint saves a new version for you.

Why do we use it?

1. It protects our work

Mistakes happen—files get overwritten, parts get deleted, or something breaks. Version control lets us go back to any previous version instantly and restore it if we need to.

2. It supports collaboration

Several people can work on the same file at the same time without overwriting each other's changes. The system helps bring everyone's updates together neatly and clearly.

3. It improves transparency

Every change is recorded automatically, including:

1. What changed
2. Who made the change
3. Why the change was made (if the person making the change makes a note)
4. When it was made

This reduces confusion and improves accountability.

4. It reduces risk

By keeping a full history, version control ensures:

- Nothing is ever lost
- Work can always be restored
- Changes can be reviewed before being accepted
- Projects remain consistent and organised

Benefits for SCC

Version control helps us work faster, safer, and more confidently—whether we're updating documents, managing data, or developing digital tools. Benefits include:

- Higher quality outputs through review and traceability
- Better teamwork across departments
- Reduced duplication and fewer conflicting edits
- Improved compliance through clear audit trails
- Lower risk of data loss or accidental overwrites

Draft documents

Many documents go through several draft stages before they are finalised or approved. Draft versions are a normal and important part of working collaboratively, but they must still be managed properly to avoid confusion, duplication, or the accidental use of incorrect information.

Draft documents should:

- be created and stored in approved shared systems (such as SharePoint or Teams)
- be managed using version control so that changes are tracked automatically
- be clearly identifiable as drafts, particularly where a document may later become a formal record

Using version control means staff do not need to create multiple separate draft files (for example “Draft v1”, “Draft v2”, “Final final”). Instead, a single document can be developed over time, with SharePoint retaining a clear history of all versions, edits, and contributors.

Further guidance on identifying, managing, and disposing of draft documents is provided further down this part.

Please see [Appendix F](#) for a step-by-step guide on how to use version control in SharePoint correctly.

Purview labels

When creating documents, staff will be asked to choose a sensitivity label that reflects how sensitive the information is.

The labels will reflect SCC’s classification guidance which uses Red, Amber and Green levels to help staff make this decision. See [Appendix C](#) for a copy of the classification guidance.

These labels help Microsoft Purview automatically protect information in the right way, for example by limiting who can access it or how it can be shared.

Applying the correct label helps ensure information is handled safely and appropriately from the start.

Reliability of records

A reliable record is one that is accurate, complete, and provides sufficient content and context to demonstrate how a decision was reached or a position was formed.

It should enable someone with no prior knowledge of the subject, work, or event to understand what happened, why it happened, and who was involved.

Staff should ensure that information is captured clearly and objectively at the time the activity takes place, ensuring that key facts, decisions, actions, and outcomes are recorded correctly.

Duplicates and drafts

Draft and duplicate information should be actively managed to reduce risk and avoid confusion.

Draft documents should be clearly marked using watermarks such as “Draft” or “Working Version”, and version control should be applied where appropriate.

Once a document has been finalised, approved, and saved in the correct corporate location, superseded drafts and unnecessary duplicates should be deleted in line with retention guidance.

Routine exchanges and minor iterations should be captured within a single email thread rather than retaining separate copies of each draft, with the final agreed decision or version clearly identifiable as the authoritative record.

Accessibility

Information and records must be created, stored and managed in a way that ensures they are accessible, usable and retrievable by staff who need them to carry out their roles.

Appropriate access controls must be in place to ensure that information and records are only accessible to authorised staff and to effectively prevent unauthorised access. See [Appendix G](#) which outlines how to manage Teams access.

Information governance considerations apply to all record formats, including paper, digital, video and audio recordings, which must be capable of being accessed, understood and, where necessary, reproduced.

Audio records should be capable of being transcribed where required to support accessibility and disclosure, and video records must allow for appropriate redaction techniques, such as pixelation or blurring, to protect third-party or exempt information.

Records must be organised and maintained so that they can be located promptly and provided in a readable and appropriate format for legal and regulatory purposes, including potential disclosure under Subject Access Requests (SARs), Freedom of Information (FOI) requests, or other statutory obligations.

Storing information

Electronic SCC information and records must be stored in approved corporate systems such as SharePoint, Teams, OneDrive or line-of-business applications (such as LiquidLogic), where they can be managed securely, retained appropriately, and accessed when needed. See [Appendix H](#) for a summary table of what to store where, and when.

1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page **23** of **63**

Email and Outlook are communication tools, not file storage systems, and should not be used to hold information on a long-term basis.

Important information contained in emails that evidence decisions, actions or service delivery must be saved into an appropriate corporate system and managed in line with retention, security and records management requirements.

Keeping information out of inboxes reduces risk, improves findability, and supports compliance with legal and audit obligations.

If an email matters, save it. If it doesn't, delete it.

Physical records that are not being used by services should be stored at the Records Management Centre. See [Part 5: Management of physical \(paper\) records](#) below for more detailed guidance on management (including storage) of physical information.

Top tips for storing information properly

- ✓ Save important emails into SharePoint, Teams, Liquid Logic, or relevant business system
- ✓ Store records where others can access them when needed rather than keeping them in personal inboxes, or One Drive
- ✓ Use links instead of attachments when sharing documents so there is one version available to everyone
- ✓ Apply appropriate naming conventions and version control once information is saved to a shared system
- ✓ Delete emails once they are no longer needed
- ✓ Physical records that are not in use by services should be stored at RMC

✗ Do not use Outlook or email inboxes as long-term storage – they are communication tools, not record-keeping systems

Retention

Keeping records for longer than we need to can cause significant problems when it comes to storage and management so it is important to make sure that records are reviewed regularly so that when they reach their retention limit, they can be assessed and a decision made about whether they should be permanently deleted or, whether there are other actions that would be more appropriate.

Statutory retention periods

Much of SCC's information is subject to statutory retention periods, i.e. there is a piece of law which says that certain types of records must be kept for a specified period of time, for example Finance and HR records are typically kept for six years, plus the current financial year.

Corporate retention periods

In the absence of any statutory retention period, there may be a corporate retention period. Details of retention periods that apply to council information can be found in the Register of Datasets.

How to set a retention period

In the absence of either statutory or corporately defined retention periods, it is down to individual services to set their own retention periods.

A retention period should indicate the length of time information should be kept for in relation to its business value, along with a trigger point, which is the point at which the retention period begins.

The key considerations when looking to implement a retention period are:

- Why the information was collected in the first place
- What business need is there to retain the information?
- Are there any follow-up process that need to be considered, for example, is there a complaint or appeal process that could be triggered that needs to be accounted for?

For some example retention periods, please see [Appendix I](#).

LG Inform+

LG Inform+ is a service that has been set up especially for local government which provides a range of tools and services, including a comprehensive list of guideline retention periods for different types of records that are likely to meet business needs.

SCC subscribes to LG Inform+ so all staff can access the Records Retention Guidance by signing in with their SCC email address and creating an account.

Please see [Appendix J](#) for a step-by-step guide to using LG Inform+ to research guideline retention periods for records.

Reviewing records when they reach their retention date

At the end of their retention period, records must be formally reviewed to determine whether they should be securely disposed of, retained for a further defined period, or preserved as part of SCC's permanent archive.

This review ensures that information is not kept longer than necessary, supports compliance with legal and regulatory requirements, and helps manage storage responsibly across all information formats.

During the review, staff should consider the record's ongoing business value, legal or statutory obligations, historical significance, and any pending information requests or audits.

Completing this process consistently ensures that SCC maintains accurate, accountable, and efficient information management practices.

Disposal of records

When records have reached the end of their retention period and no longer hold operational, legal, financial, or historical value, they should be securely disposed of.

Disposal must always be carried out in line with SCC's information governance and security requirements to ensure that personal, confidential, or sensitive information is irretrievably destroyed.

Approved disposal methods include secure shredding for paper records and certified digital deletion for electronic files.

Proper disposal prevents unnecessary accumulation of outdated information, reduces storage costs, and mitigates the risk of inappropriate access to obsolete data.

Archiving of records

Records that continue to hold long-term business, legal, or historical value after their retention period expires should be transferred to Suffolk Archives.

Archiving ensures that significant records are preserved in a controlled environment where they remain accessible, protected, and usable for future reference, research, or statutory purposes.

During the archiving process, records must be assessed for completeness, labelled appropriately, and accompanied by sufficient metadata to support retrieval and context.

Archiving supports good organisational memory and maintains the public record of SCC's decisions, services, and impact.

1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page **26** of **63**

If a service believes that a record that has reached its review date might be of social, cultural or historic value, it can be offered to the Archives who will assess the record and then confirm whether or not it will form part of the Archive.

Business continuity and back-ups

Effective business continuity relies on SCC information being stored in approved, shared systems so it remains accessible when needed, regardless of staff absence or change.

Staff must ensure that records and key information are saved in appropriate corporate systems, rather than personal inboxes or local storage, so others can access them to continue service delivery.

SCC IT services run regular, automated back-ups of corporate systems, meaning staff do not need to make duplicate copies of information for back-up purposes.

In an emergency, physical information can be removed from SCC premises however, staff must ensure that appropriate security measures are taken to protect it away from SCC.

Storing information correctly reduces risk, avoids duplication, and ensures SCC can continue to operate effectively during disruption.

Part 5: Management of physical (paper) records

Although SCC carries out the vast majority of its work electronically, SCC continues to hold a significant volume of physical (paper) records.

These records remain subject to the same legal, regulatory, and governance requirements as electronic records and must be managed carefully throughout their lifecycle.

Physical records may include historic files, legacy case records, signed originals where a wet signature is required, or records that have not yet been digitised. Where physical records exist, services must ensure they are created, stored, accessed, retained, and disposed of securely, and in line with SCC policy.

The principles set out in this handbook apply equally to physical and electronic records. Physical records should only be created or retained where there is a clear business, legal, or operational need.

Where possible, services should consider digitisation to reduce storage burdens, improve accessibility, and support business continuity—subject to data protection, retention, and business requirements.

Physical records must:

- be clearly identifiable and appropriately labelled
- be stored securely and protected from damage, loss, or unauthorised access
- have an assigned retention period
- be reviewed, disposed of, or archived in line with SCC retention guidance

Creating physical records and information

Physical records should only be created where there is a genuine requirement to do so. Examples may include signed legal documents, records received in paper format from external bodies, or historic documentation that has ongoing value.

When creating or receiving physical records, staff must:

- ensure the record is complete, accurate, and legible
- apply the correct information classification (Red, Amber, or Green)
- avoid creating duplicate paper copies where an electronic version already exists
- ensure a clear link exists between physical records and any related electronic records, where relevant

Physical records that form part of an ongoing business process should not be treated as informal or unmanaged simply because they are paper-based.

Storage of physical records

SCC has its own Records Management Centre (RMC), located at Gatacre Road in Ipswich, which provides secure, controlled storage for physical records requiring medium to long-term retention. The RMC includes strong rooms with environmental conditions suitable for the long-term preservation of records.

Because of this, it is recommended that all physical records are stored at RMC when they are not in use by services. This ensures that records are subject to appropriate security measures and reduces the risk of information and records being lost.

Physical records must not be stored in unsuitable locations for their sensitivity such as:

- unlocked cupboards or open office areas
- staff homes, unless formally approved and risk-assessed
- uncontrolled storage rooms or basements
- vehicles or temporary locations for longer than absolutely necessary

Services are responsible for ensuring that:

- records are transferred to approved storage location, i.e. RMC when no longer required for day-to-day use
- appropriate inventories or tracking information is maintained
- access is restricted to authorised staff only

Whilst physical information is in use by service, then staff should ensure that it is kept securely when it's not being used, for example, in lockable and locked filing cabinets.

Access, movement, and tracking of physical records

Access to physical records must be on a need-to-know basis and consistent with the record's classification and sensitivity. Any removal, loan, or movement of physical records should be controlled and recorded to maintain accountability and reduce the risk of loss or unauthorised access.

Services should ensure that:

- records are signed in and out when removed from storage
- files are returned promptly when no longer required
- any loss, damage, or unauthorised access is reported immediately in line with SCC incident management procedures

Working away from the office

Where staff are required to work away from the office and need access to physical records, this must be carefully managed. Physical records should only be taken off-site where necessary and with appropriate safeguards in place.

When working remotely with physical records, staff should:

- log records as they are removed from SCC premises and sign them back in on return
- transport records securely and discreetly
- ensure records are not left unattended in public or shared spaces
- store records securely while off-site
- return the records to approved SCC storage as soon as possible

Physical records containing personal, confidential, or sensitive information must never be left unsecured or accessible to unauthorised individuals. Any loss, delay, or unauthorised access while working off-site must be reported immediately in line with SCC's Information Security Incident Management process.

Retention, review, disposal, and archiving of physical records

Physical records are subject to the same retention and disposal requirements as electronic records. When a physical record reaches the end of its retention period, it must be formally reviewed to determine whether it should be securely destroyed, retained for a longer period, e.g. for administrative use or updated retention guidance, or transferred to Suffolk Archives.

For records stored at RMC, the RMC team will co-ordinate the review process and contact information owners when records reach their review date. Services must respond promptly to review requests so that records can be securely destroyed, retained lawfully, or transferred to Suffolk Archives where appropriate.

Keeping records for longer than necessary is one of the most significant information risks to SCC and must be actively avoided.

Secure disposal methods must be used at all times, such as using the blue confidential shredding bins that are found on every floorplate in SCC buildings. Records identified as having long-term historical, legal, or cultural value should be offered to Suffolk Archives in line with council procedures.

Part 6: Security

Information security is a fundamental requirement of data protection law and requires that appropriate technical and organisational measures are applied to protect information. These measures must be proportionate to the sensitivity and risk associated with the data being handled.

In practice, this means that the more sensitive the information, the greater the level of care, control, and protection that must be applied to ensure it is kept secure from unauthorised access, loss, or misuse.

SCC has a range of organisational and technical security measures in place to support the protection of its information and systems. These include:

- the use of unique user account IDs and strong passwords
- the use of encrypted devices only on SCC's network
- appropriate firewalls and virus detection software

These all help to ensure accountability and prevent unauthorised access.

Physical security measures are also in place, such as:

- card-controlled access to buildings and offices
- the provision of blue confidential waste bins for the secure disposal of sensitive paper records
- its clear desk policy

In addition, follow-me printing is used to ensure documents are only printed when the authorised user is present, reducing the risk of information being viewed or taken by others.

Staff must use these controls appropriately and consistently however information is being used, to help maintain the security of SCC information.

Failure to follow these requirements may result in security incidents, data breaches, and potential disciplinary action.

Cyber security and awareness

All staff must remain vigilant to the risk of phishing emails, scams, and other malicious activity.

Suspicious emails may attempt to trick users into revealing information or clicking unsafe links, often by creating a sense of urgency or appearing to come from a trusted source.

Staff should not click on links or open attachments unless they are confident the source is legitimate and should report any suspicious messages to the IT Service desk, without forwarding any suspicious communications.

Users must not download software or applications from the internet unless they have been approved by IT, as this can introduce security risks such as malware.

Awareness of common phishing tactics and taking a cautious approach to unexpected communications are essential to protecting SCC systems and information.

How to share and transfer information securely

All SCC information must be shared and transferred in a secure and controlled manner to protect confidentiality, integrity, and maintain compliance with SCC policies.

For physical records, appropriate safeguards must be in place, including the use of Royal Mail “Signed For” or “Special Delivery” services where required, and arranging secure collection with SCC’s courier service with verification of identification for sensitive materials. Documents should be clearly addressed and packaged to prevent unauthorised access.

The level of service used must reflect the sensitivity of the information.

For electronic information, data must be transmitted using secure channels, with emails appropriately classified and protected using Microsoft Purview sensitivity labelling.

Where possible, approved secure transfer methods such as Safedrop or authorised customer portals must be used in place of standard email attachments, particularly for sensitive or personal data.

These controls help ensure that information is only accessible to authorised recipients and remains protected throughout its transfer.

A key takeaway before sending any SCC information is to:

- pause before sending
- double-check the recipient’s contact details carefully
- ask yourself, does the recipient need this – if not, don’t send it

Removable devices (including charging personal devices)

All removable storage devices used on SCC networks and machines must comply with strict security requirements to protect organisational data.

SCC-issued devices and removeable storage (including laptops, tablets, USB drives and mobile phones) must be encrypted as standard using BitLocker to ensure that any data stored is safeguarded against unauthorised access.

Under no circumstances should encryption passwords or recovery keys be stored with the device itself or with associated equipment (including laptops), as this creates a significant security risk.

Users are responsible for the secure handling of removable media throughout its lifecycle and must return devices to IT at the end of their life for secure destruction and appropriate data sanitisation. Failure to adhere to these controls may result in disciplinary action and potential data breach implications.

Charging of personal devices within SCC premises must be carried out using designated mains power sockets only. Under no circumstances should personal devices be connected to SCC laptops, docking stations, or workstation USB/USB-C ports for charging purposes.

This restriction is in place to minimise security risks such as unauthorised data transfer, malware introduction, and potential compromise of SCC systems and networks. Adhering to this control helps ensure the integrity and security of SCC equipment and information assets.

Using information away from the office

When working remotely or away from the office, all staff must ensure that the same information security standards are maintained as if they were working on SCC premises.

General Principles

The same rules for handling information apply regardless of location.

Staff are responsible for ensuring that information remains secure, confidential, and protected from unauthorised access at all times.

Physical Information

Any physical information removed from SCC premises must be formally signed out and signed back in in line with local procedures.

Documents must be kept secure at all times, including:

- Stored in a lockable cabinet or drawer when not in use
- Kept out of sight and away from general view in both work and home environments

Physical information must never be left unattended in public or unsecured locations.

1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page **33** of **63**

Electronic Information and Devices

Devices (e.g. laptops, tablets, USB drives) must be kept secure and under the user's control at all times.

Devices must not be left in vehicles overnight or for prolonged periods.

Screens should be positioned to prevent unauthorised viewing ("shoulder surfing"), particularly in public or shared spaces.

Working in Public Places

Care must be taken when working in public environments (e.g. trains, cafes, shared spaces).

Staff must not access RED-level or highly sensitive information in public places, due to the risk of unauthorised viewing or discussion being overheard.

Conversations involving sensitive information should not take place where they may be overheard.

Additional Good Practice

Always lock your device when not in use.

Use secure networks wherever possible; avoid public Wi-Fi unless through approved secure connections.

Immediately report any loss, theft, or suspected compromise of information or devices.

Studying at SCC

If you are studying as part of your role within SCC and are required to submit assessments for marking, you must ensure that you understand the expectations set by your training provider.

Where this involves compiling a portfolio of work undertaken at SCC, all information must be handled in line with data protection and information governance requirements.

Case studies and examples must be appropriately anonymised, and identifiable personal or confidential information must never be shared. This ensures that SCC information, service users, and colleagues remain protected at all times.

Third-party access to SCC information and systems

Third-party access to SCC systems and information must be appropriate, proportionate, and formally authorised by the relevant manager before it is granted.

Access should be limited to what is necessary for the third-party to carry out their role and must be monitored and reviewed regularly.

SCC expects third parties to meet the same standards of information security and data protection as its own staff, ensuring that all information is handled, stored, and processed in a secure and compliant manner in line with SCC policies and legal requirements.

Reporting information security incidents and personal data breaches

All staff must report any information security incidents and potential personal data breaches as soon as they are identified, using the IT Self Service system.

Prompt reporting enables SCC to assess risks, take appropriate action, and meet legal and regulatory requirements.

Staff are expected to fully engage with any subsequent investigation, including providing relevant information and cooperating with Information Governance and IT teams.

Early reporting and cooperation are essential to minimising impact and ensuring lessons are learned.

Part 7: Resources

Policies

[Acceptable Use of Information and Systems](#)

[Records Management](#)

Guidance – including online platforms and tools

[Register of datasets](#)

[Register of DPIAs](#)

[Privacy notices](#)

[Online tools and platforms](#)

[Information classification](#)

Resources

[LG Inform+](#)

[Records Management Centre](#)

1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page **36** of **63**

Appendix A – Examples of records and non-records

The table below sets out examples of records that SCC holds and creates, as well as some examples of pieces of information that do not equate to a record.

Please note that these lists are not exhaustive.

<i>Examples of records</i>	<i>Examples of non-records</i>
Emails that document decisions, instructions, approvals, or actions taken as part of council business	Convenience copies or duplicates kept only for reference and not needed as evidence of activity
Documents created or received as part of delivering services (e.g., reports, assessments, meeting notes, case-related information)	Drafts that have been superseded by a final approved version and do not contain unique decision-making information
Information captured in approved systems (e.g., datasets, logs, or forms) that evidences operational activity or service provision	Personal notes, reminders, or working materials not used to record decisions or official activity
Records that provide evidence of decisions, advice, or actions (including approvals, instructions, or audit trails)	Transient communications such as meeting invites, simple acknowledgements, or notifications with no lasting business value
Contract, procurement, and financial records that evidence expenditure, commitments, approvals, or delivery of council services	External reference material (e.g., guidance from other organisations, news articles, research material) that does not document SCC business

Appendix B – Summary of responsibilities

Responsibility	Managers	Staff
Leadership and culture	Provide clear leadership, set expectations, and model good practice in records management.	Follow the practices and expectations set by management and SCC policies.
Creating and capturing records	Ensure teams create accurate, reliable records and capture them in approved systems.	Create complete, accurate records and store them in approved corporate systems.
Compliance with legislation and policy	Ensure service complies with data protection, FOI/EIR, and internal policies; ensure staff receive training.	Handle information in line with data protection, FOI/EIR, and SCC internal policies.
Information security and access	Ensure staff apply RAG classification; review permissions; maintain secure handling.	Apply correct classification, restrict access appropriately, report security concerns.
Storage of information	Ensure information is stored in correct locations and formats.	Store records only in approved systems and ensure physical/digital storage is appropriate and secure.
Retention and disposal	Ensure accurate retention periods; oversee review and secure disposal/archiving.	Follow retention rules; review, dispose, or archive records securely.
Version control and collaboration	Promote good version control; ensure teams use SharePoint features.	Use naming conventions and version control features.
Business continuity	Ensure key records are backed up, accessible, and support continuity.	Ensure essential information is stored in shared systems.
Risk management	Identify and mitigate information-related risks.	Report concerns about poor practice, missing data, or incorrect storage.
Training and support	Ensure staff receive appropriate training and understand obligations.	Participate in training and seek guidance when unsure.
Assurance and quality control	Conduct checks, address poor practice, and support statutory requests.	Ensure records are accessible and accurate to support requests.

1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page **38** of **63**

Appendix C – SCC information classification guidance

The purpose of this guidance is to classify all written, spoken and technological information by its sensitivity so that you can decide the appropriate measures you need to take to protect it.

SCC uses a traffic light rating system (i.e. Red, Amber, Green) to identify the sensitivity of its information. Please see the table below for information to help you classify the data you are working with:

SCC classification levels	Definition	Examples of information
RED	Information which poses high risk to privacy. This could include: information about an individual's ethnicity • political opinions • religious or philosophical beliefs • trade union membership • genetic data • biometric data where it is used to identify people • sex life and sexual orientation • gender reassignment • criminal offence data • health information	• Health & Social Care records • Financial information • Employee data • Health, safety and wellbeing • Corporate information e.g. information which would have a significant impact on the reputation or business of SCC
AMBER	Information which poses little or no risk to an individual's privacy. N.B. It should be noted that if the information is contained within a RED level document, or if you are using large volumes	• Business contact information including email addresses, postal addresses and phone numbers • Customer names and addresses

1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page **39** of **63**

	of AMBER level data, it should be treated as RED level data – see above	• Unique identifiers such as NHS numbers, NI numbers, case management system ID numbers, e.g. Liquid Logic
GREEN	Information which poses no risk to privacy	• Information that would be disclosed under a Freedom of Information (FOI) or Environmental Information (EIR) request • Information that is routinely published, e.g. staff salaries, statements of accounts, Cabinet meeting minutes

Appendix D – Online tools and platforms guidance

SCC is increasingly moving towards on-line data collection, consequently it is important to understand what types of data (e.g. nonpersonal, personal, sensitive data) can be processed via its on-line data collection tools and platforms.

This guidance sets out the online data collection tools and platforms which can be used for data collection and explains what type (level) of data can and cannot be processed via them.

The guidance also includes data management information for services to ensure that information collected via SCC's on-line tools and platforms is appropriately managed. For more information about records management, see SCC's Records Management Policy.

For further information about public-facing SCC websites, mobile apps, online forms, including customer portals, online transactional services where people use forms to report issues, make payments, submit requests and applications, see SCC's Websites, Online Forms and Mobile Applications policy.

On-line tools and platforms	Suitable for	Not suitable for	Data management
SCC website	Publishing public information which includes Green level information only.	Red and Amber level information.	Directorates/services are responsible for regularly reviewing and ensuring that the content of their externally published information is kept up to date.
IRIS intranet	Staff information which includes Green and Amber level information which poses little/no risk to privacy (e.g. SCC staff contact details, external generic contact details).	Red level and Amber (e.g. non-generic external contact details) level information.	Directorates/services are responsible for regularly reviewing and ensuring that the content of published information is kept up to date.

1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page **41** of **63**

MS Teams	Short term collaboration, e.g. specific projects, via chat messages, meetings, sharing documents, calendar, Tel calls, which may include Red, Amber, and Green level information.	N/A	Data stored in MS Teams is subject to organisational retention policies as outlined in Information Management This means that MS Teams is not suitable for the storage of client data and case records. All documentation which requires longer term retention should be transferred to the relevant SharePoint site within a service specific agreed timeframe. Services should, prior to any transfers of information to SharePoint, consider data minimisation (e.g. is it necessary to keep all of the data for storage purposes?).
SharePoint	Primary online storage system for information making it easy to collaborate with both internal and approved external colleagues. Information which includes Red, Amber, and Green level data can be stored on SharePoint.	N/A	Shared drives must not be migrated to MS Teams. Services should, prior to any transfers of information to SharePoint, consider data minimisation (e.g. is it necessary to keep all of the data for storage purposes?). Services should also ensure that SharePoint sites are marked as

1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page **42** of **63**

			Private rather than Public where relevant, and that stored documents have appropriate access allocated to them so that only authorised personnel can view them.
OneDrive	Personal storage space. OneDrive can be used to store your personal, work-related documents (e.g. PDRs) as well as being used for short term storage of files which may be needed offline or whilst creating documentation which is not ready for publication or wider sharing. You can collaborate with internal colleagues on OneDrive files. Information which includes Red, Amber, and Green level data can be stored on SharePoint.	N/A	Once non-personal work-related documents are final, they must be moved to SharePoint or MS Teams. Services should, prior to any transfers of information to SharePoint or MS Teams, consider data minimisation (e.g. is it necessary to keep all of the data for storage purposes?). Services should also ensure that SharePoint sites are marked as Private rather than Public where relevant, and that stored documents have appropriate access allocated to them so that only authorised personnel can view them.
Microsoft forms	Creating and sharing surveys, quizzes, and polls. Green and Amber level information which poses little/no risk to privacy (e.g. business email address, partial	Red and Amber level data which poses a greater risk to privacy (e.g. full name, date of	Information collected via a Microsoft form must be promptly transferred (e.g. within 72 hours of receipt) to the service's permanent storage system and the form containing the

1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page **43** of **63**

	postcode). If you are already using MS forms for the collection of Red or Amber level information, please contact your Directorate's SIA for further advice. For example, the service may need to check/update an existing DPIA to ensure its use of MS forms and data management processes are recorded in it. For further advice about using other secure on-line data collection tools, services should contact serviceimprovement@suffolk.gov.uk.	birth, address, contact details, health and care, financial data.).	information must be securely and permanently deleted.
Goss forms	Customer-facing online forms, which enable payments and transactions and manage internal workflow and customer data. Customers are also able to create and manage their accounts. Information which includes Red, Amber, and Green level data can be processed via the Goss platform. Note: there is a significant backlog of requests for GOSS provision which means that requests are	N/A	Directorates/services to work with the Service Improvement team to: • specify the data that must be collected by the online form • to test the new online service and approve this for going live. A GOSS Request Form must be completed and approved before the new service can 'go live.' The Request Form must specify the data retention period for the

1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page **44** of **63**

	managed on a priority basis. Services wishing to use GOSS must ensure they have contacted the Service Improvement team as part of their project planning.		information collected via GOSS which will be applied and automatically managed by the system.
PowerApps	Creation of bespoke user defined applications to meet niche business requirements which are not covered by any existing products and services. Requires development and in some cases additional knowledge or skills to operate. Red, Amber, and Green level data can be processed, but Red and Amber level data can only be processed if the system used to store Power Automate generated data is one of the other systems defined in this Guidance as suitable for Red and Amber level data.	N/A	This product can integrate to any Microsoft service and also to limited third-party services. The system used for storing Power Automate generated data must be one of the systems defined as suitable for storing Red and Amber level data in this guidance.
Power Automate	Creation of bespoke user defined applications to meet niche business requirements which are not covered by any existing products and services.	N/A	This product can integrate to any Microsoft service and also to limited third-party services. The system used for storing Power Automate generated data must be

1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page **45** of **63**

	Requires development and in some cases additional knowledge or skills to operate. Red, Amber, and Green level data can be processed, but Red and Amber level data can only be processed if the system used to store Power Automate generated data is one of the other systems defined in this Guidance as suitable for Red and Amber level data.		one of the systems defined as suitable for storing Red and Amber level data in this guidance.
Mobiles and messaging apps (e.g. WhatsApp, SMS, Facebook Messenger, Viber, Signal)	Instant communications which include Green and Amber level information which poses little/no risk to privacy (e.g. confirmation of meeting date, time, and location (partial postcode or town only)).	Red level and Amber level information (e.g. information which could pose a risk to privacy such as full name, date of birth, full details of location, reason for meeting).	Customer communications must be promptly transferred to the service's permanent storage system and the information permanently deleted from the mobile/app within, for example 24 hours). See Appendix C in the Acceptable Use policy for guidance in relation to WhatsApp data management.
Contensis (Zengenti)	Simple web forms capturing Green and Amber level data (e.g. customer names, email addresses, contact details).	Red level data (any online service requiring sensitive customer data is signposted to an alternative option).	Data collected and stored securely in the Contensis CMS accessed only by platform admins, data also managed by service owners of the forms.

1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page **46** of **63**

Appendix E – Naming convention guidance

This appendix provides guidance and practical examples to support consistent file and folder naming across SCC.

Although there is no corporately prescribed naming convention within SCC, consistent naming conventions improve information governance, accessibility, version control, and compliance with records management and data protection requirements.

1. Core Principles for Naming

All SCC file and folder names should be:

- clear – instantly understandable without opening the file
- consistent – named using the same structure across teams
- searchable – easy to locate using system search tools
- chronologically sortable – files naturally sort in time order
- appropriate – do not personal data or sensitive information in names

2. Using Dates for Chronological Sorting

Recommended date format - all file and folder names that include dates should use the following format:

YYYY-MM-DD

Using YYYY-MM-DD aligns with international standards¹ and provides several key benefits:

- Automatic chronological sorting - when files are listed alphabetically, they will also appear in date order (oldest to newest)
- Consistency across SCC systems - works reliably in SharePoint, OneDrive, network drives, and other SCC platforms
- Reduced ambiguity - avoids confusion between UK and US date formats (e.g. 03/04/26)
- Improved records management - supports retention schedules, audits, and lifecycle management
- Long-term clarity - dates remain understandable regardless of when or where the file is accessed

¹ ISO 8601

1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page **47** of **63**

Formats to avoid:

- 05-05-26
- 05_05_2026
- May 5th 2026
- 05May26
- 2026.05.05

These formats:

- Do not sort correctly
- Can be misinterpreted
- Are inconsistent across teams and systems

3. Standard File Naming Structure

Where possible, file names should follow this order:

YYY-MM-DD – Subject or description (brief) – version (if needed)

Good practice	Explanation
2026-05-05 – Team meeting minutes	Sorts chronologically, clear purpose
2025-11-01 – Data sharing agreement v1.0	Clear date, document type and version
2024-03-15 – Training attendance register	Easy to identify without opening

4. Version Control

When multiple versions exist, include a clear version number at the end of the file name (see Appendix F below for more details about version control). For example:

- 2026-04-12 – Privacy Notice – v1.0
- 2026-04-12 – Privacy Notice – v1.1
- 2026-04-12 – Privacy Notice – FINAL

Avoid vague terms such as:

- latest
- new
- amended

5. Folder Naming Guidance

Folder names should also follow clear and consistent conventions.

1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page **48** of **63**

Date-led folders (where applicable) - used for items such as meetings, projects, or audits:

- 2026-01 Fraud investigation
- 2026-03 Audit evidence

Non-date folders - for ongoing or reference content, use descriptive names without dates:

- Policies and Procedures
- Templates
- Training Materials

6. Characters and Formatting

Do use	Avoid the use of
Letters and numbers	Special characters (? :*?"<>)
Spaces, hyphens or underscores	Excessive underscores
	Long file names

7. Data Protection Considerations

File and folder names should not include:

- Names of service users
- NHS numbers, NI numbers, or other identifiers
- Special category personal data

This reduces the risk of data exposure and supports SCC's data protection and records management obligations.

Summary

Using consistent, date-led naming conventions:

- makes information easier to find
- reduces duplication and errors
- supports compliance and governance
- saves time for everyone

All SCC staff should apply this guidance when creating or saving files and folders.

Appendix F - How to use version control in SharePoint

Step 1: Make sure versioning is turned on

SCC has it enabled by default. To check (requires library admin permissions):

- Go to the document library
- Select Settings → Library Settings
- Choose Versioning Settings
- Confirm that Major Versioning or Major + Minor is enabled

Step 2: Upload or open your file

You can:

- Upload a document
- Create a new one directly in SharePoint (Word, Excel, PowerPoint, OneNote)
- Or open an existing file and start editing

SharePoint will track every save automatically — you don't need to do anything special.

Step 3: Edit as usual

When you:

- Edit in Word/Excel/PowerPoint Online
- Edit in desktop apps (as long as autosave is on)
- Sync using OneDrive

SharePoint automatically creates a new version each time you save.

Step 4: View previous versions

This is the most useful part. To see the full version history:

- Hover over the file
- Click the three dots (...)
- Select Version History

You'll see:

- The date & time of each version
- Who made the change
- Comments (if any)
- Whether it was major or minor**
- The option to restore, delete, or open each version

Step 5: Restore an older version (time machine mode)

- Open Version History
- Hover over the version you want
- Click the arrow beside it
- Choose Restore

This instantly rolls the file back — but don't worry, SharePoint keeps *another* version of the restored version. Nothing is lost.

Step 6: Compare versions (for Word docs)

Open the file in Word Online or Word Desktop and choose:

- Review → Compare

SharePoint provides a comparison showing:

- Added text
- Removed text
- Formatting changes
- Who made each change

This is brilliant for tracking team contributions.

Step 7: Add version comments (optional but useful)

When you check in or save major changes, you may be prompted to add a comment.

Examples:

- “Updated data set for January”
- “Revised policy wording based on Legal review”
- “Fixed errors in the table formulas”

These appear in the version history and help reviewers understand the change.

Optional: Check In / Check Out (for controlled editing)

You may want to use this if:

- Only one person should edit the file at a time
- You want to avoid clashing edits
- You need to force people to leave comments

To check out:

- Click ...
- Choose **Check Out**

To check in:

- Click ...
- Choose **Check In**

1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page **51** of **63**

- Add a comment (recommended)

To discard Check Out:

If you change your mind: ... → **Discard Check Out**

****Major and minor versions in SharePoint**

SharePoint uses major and minor versions to track changes throughout a document's lifecycle. This helps ensure accuracy, transparency, and accountability when creating, reviewing, and publishing records.

Major versions (e.g., 1.0, 2.0, 3.0)

Major versions represent significant updates or milestones, such as when a document is published, approved, or otherwise finalised for wider use. They appear as whole numbers (1.0 → 2.0 → 3.0). These versions mark key points in a document's evolution and are typically used when the content is ready to be shared beyond its immediate editors.

Minor versions (e.g., 1.1, 1.2, 1.3)

Minor versions capture smaller, iterative changes made while a document is still being developed or reviewed. They are used for drafts and internal amendments before a document reaches a major milestone and appears as decimal increments (1.1 → 1.2 → 1.3). Minor versioning is particularly helpful for teams working collaboratively, as it preserves every edit made before formal publication.

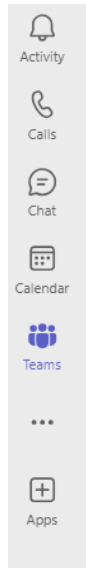
How they work together

During drafting, SharePoint will record each change as a minor version, allowing teams to refine content without prematurely marking it as final. Once the document is approved or reaches a significant stage, it is saved as a major version, providing a clear audit trail of published updates. This versioning structure supports robust records management, ensuring clarity over what constitutes a finalised document versus work in progress.

Appendix G – How to check access permissions on Teams

To check access permissions on a team site, please follow the steps below:

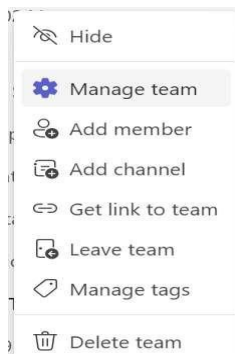
1. To view teams that you are a member of, open Microsoft Teams and select the Teams icon on the left-hand menu. N.B. Only team owners will be able to change permissions.



2. Hover over the name of your team site in the list of teams on the left-hand side of your screen and click on the three dots.

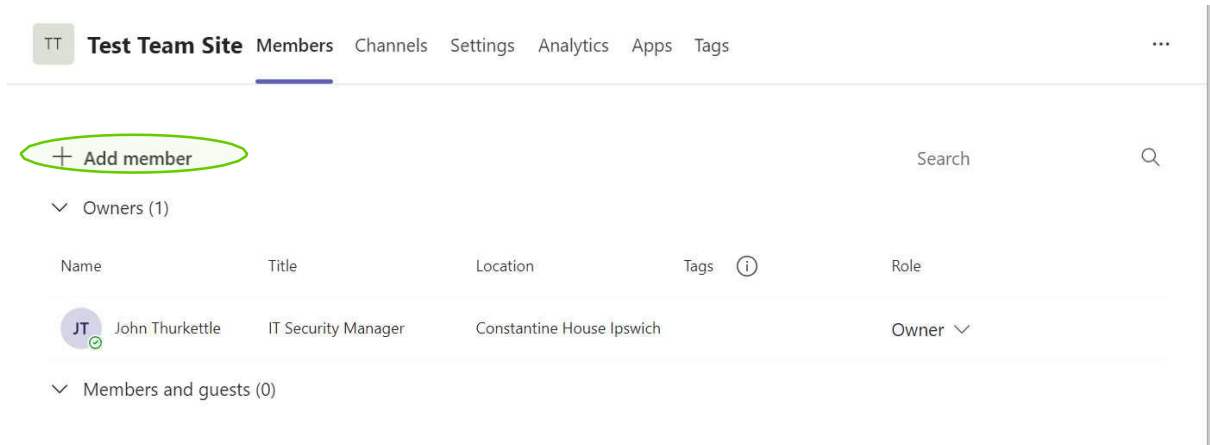


3. From the menu click “Manage Team”



1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page **53** of **63**

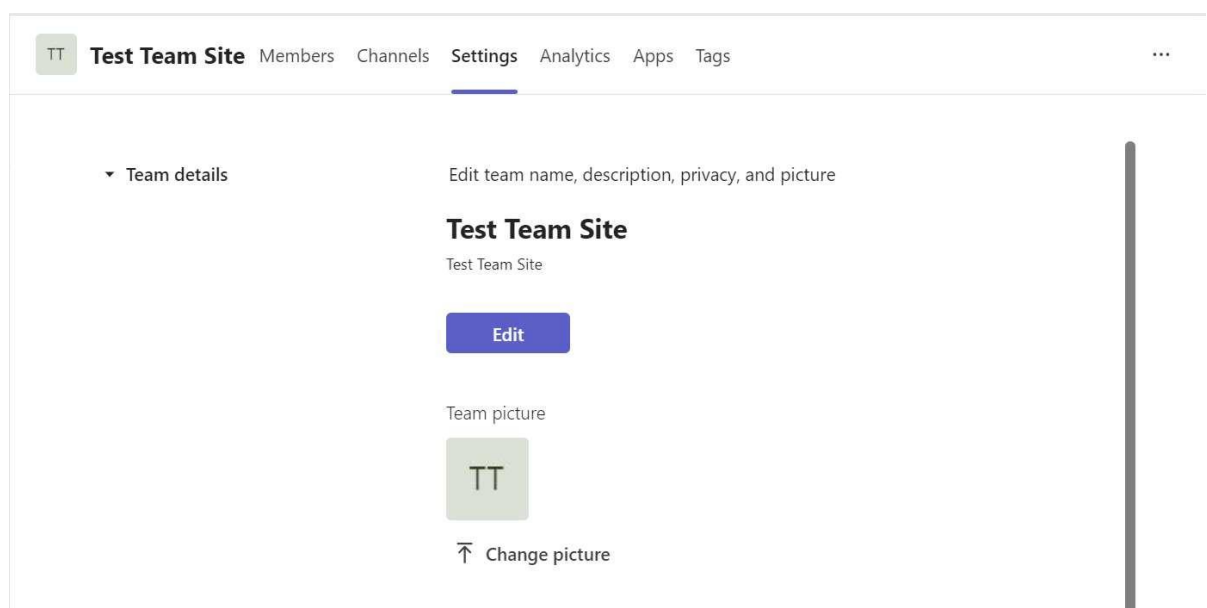
4. On this page you can see who are the site owners, and who are members - please check the members and owners list to make sure this is correct.
5. You can add new members by clicking on the “Add member” button in the top left of the page



6. You can remove existing members by selecting the cross at the end of the line where they are named

Once you have checked that the membership is appropriate, next check to see if your team site is public or private.

7. Click on the settings tab at the top of the Members page



8. Next click on the blue “Edit” button which will bring up the screen shown below. The privacy settings will show as either “Private”, or “Public” and you can change this using the drop-down options. Please check to make sure that the appropriate settings are selected, taking into consideration the nature of the information that your team site contains, i.e. personal information, red level or official- sensitive information should be set to Private.

N.B. All new Teams sites will automatically default to “Private”. If you require an existing Private group to be set to Public, please complete the following request form: [Request a Public group](#)

Edit Test Team Site team details

Collaborate closely with a group of people inside your organization based on project, initiative, or common interest. [Learn more about teams and channels](#)

Team name *

Test Team Site



Description

Test Team Site

Privacy

Public - Anyone in your organization can join



Appendix H – Where to store records

	Suitable for storing	Not to be stored here
	Official records and documents including those with meta data Files requiring digital preservation File sharing with trusted third parties Safe for Green, Amber and Red level data	Personal documentation/files Non-records
	Closed communication with a specific group of people File sharing with trusted third parties Temporary document storage Meetings with colleagues and external guests Safe for Green, Amber and Red level data	Long term file storage Managed records Long term client data and case records storage
	Personal documents Offline or off-site temporary document use on SCC hardware Drafting documents and collaborating with colleagues Safe for Green, Amber and Red level data	Long term document storage Official files Client data and case records storage
	SCC internal communications General corporate information Corporate information on directorates and roles Policy and guidance Links to corporate systems	Information intended for public consumption Amber or Red level service data
	Communications with public and partners [appropriately redacted] Public information Public Green level data	Information not intended for public consumption

1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page **56** of **63**

Appendix I – Setting retention periods

Below you will find a step-by-step approach to setting retention periods for SCC information.

Step 1: Identify the type of information.

Start by clearly identifying what the information is and why it exists. Ask yourself:

- Is this a record or a non-record?
- Does it evidence a decision, action, service delivery, or legal obligation?
- Is it personal data, special category data, or non-personal information?
- Is it linked to a specific case, project, individual, or business function?

If the information does not provide evidence of council business, it may not need a formal retention period.

Step 2: Check for existing retention requirements

Before setting a new retention period, you must check whether one already applies:

- **Statutory retention periods** - some records must be kept for a specific time under law (e.g. finance, employment, safeguarding)
- **Corporate retention periods** - may already exist so you should check SCC's Register of Datasets

If a statutory or corporate period exists, it must be followed.

You can use LG Inform+ to check retention schedules – see Appendix H below for how.

Step 3: Consider key retention factors

If no existing retention period applies, consider the following factors together:

- **Business need** - how long is the information needed to deliver or evidence the service? Is it required for ongoing reference, audit, or operational continuity?
- **Legal and regulatory risk** - could the information be needed for complaints, appeals, inspections, or legal challenge? Is there a realistic limitation period that applies?

- **Data protection principles** - is the information personal data? Would keeping it longer than necessary increase privacy risk?
- **Frequency of use** - is the information actively used, occasionally referenced, or rarely accessed?
- **Historical or long-term value** - does the information record significant decisions, policies, or impacts? Could it reasonably be of archival value?

Retention periods should always be justifiable and proportionate.

Step 4: Set a clear retention rule

Once the retention period is agreed, it must be:

- clearly defined (e.g. “6 years after case closure”)
- applied consistently
- recorded in the Register of Datasets where appropriate
- supported by a clear trigger event (e.g. closure, supersession, end of contract)

Step 5: Review and disposal

At the end of the retention period, records must be formally reviewed to decide whether they should be:

- securely destroyed
- retained for a further defined period (with justification)
- transferred to Suffolk Archives

Records, and especially personal and special category data, must not be kept indefinitely “just in case”.

Please see the table below which contains examples of recommended retention periods for different information types.

N.B. These examples are illustrative, not exhaustive. Services must always check for statutory or corporate retention periods first.

Retention periods should be:

- clearly defined
- consistently applied, and
- supported by a trigger event (e.g. closure, supersession, contract end)

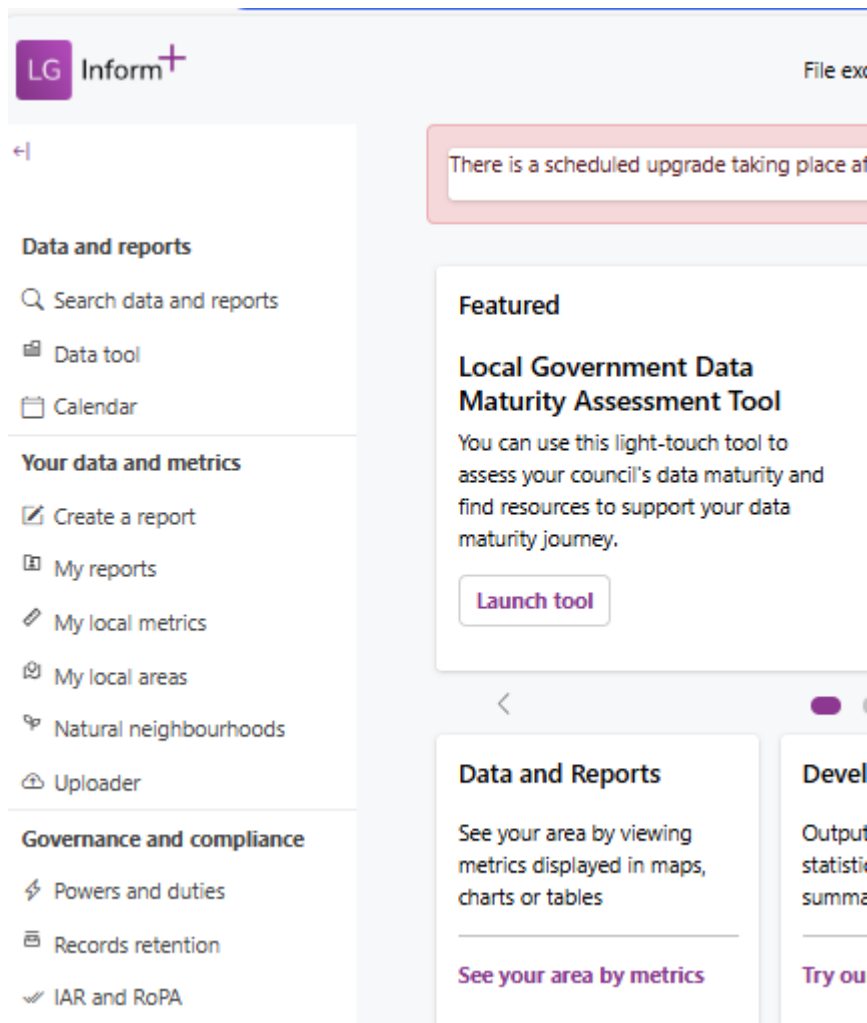
Summary table – example retention approaches by information type

Information type	Typical examples	Key considerations	Typical retention approach
Policy and governance records	Approved policies, strategy papers, decision and approval records	Evidence decision-making and accountability; may have long-term reference value	Retain while current plus a defined period after withdrawal ; consider archival value for final versions
Project and programme records	Project plans, risk logs, reports, closure documentation	Audit and assurance requirements; potential post-implementation review	Retain for a defined period after project closure ; key records often longer than working drafts
Case files and service delivery records (personal data)	Case notes, assessments, correspondence, decisions about individuals	High legal and privacy risk; often subject to statutory guidance	Retain in line with statutory or LG Inform+ guidance; retention usually triggered by case closure
Routine administrative records	Routine emails, non-decision meeting notes, working trackers	Limited long-term value; duplication common	Short retention period; dispose once superseded or no longer needed
Financial and contractual records	Contracts, invoices, payment records, procurement documents	Statutory and audit requirements; risk of challenge	Retain for defined statutory or guideline period, typically starting after contract end or financial year close
Training and competence records	Training attendance, certificates, assessments	Evidence of compliance and competence; employment considerations	Retain while relevant plus a defined period ; informal learning records usually shorter retention

1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page **59** of **63**

Appendix J – Step-by-step guide to LG Inform+ retention tool

1. From the [LG Inform+ home page](#), select “Records retention” from the menu down the left side of the screen



2. Scroll down the page to below where the filters are and you will find lists of suggested retention periods for different types of records categorised by business function

Administration and Government - Data protection and freedom of information



All records relating to the management of subject access requests under General Data Protection Regulations



All records relating to the management of Freedom of Information Requests

1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page **60** of **63**

3. You can also use the filters at the top of the page to narrow your search down to specific areas.

Filters

Hide filters ▲

Organisation type ?
County council ▼

Legal/business ?
Business ▼

Business function ?
Administration and Government, Asylum and immigration, Commercial activities, Goods and services, Procurement, Communicat ▼

Records containing ?
Special, Personal ▼

Appendix K – Top tips for good records management

Good records management is everyone's responsibility. These simple actions help keep SCC information secure, accessible, and compliant.

Area	Do	Don't
Creating records	Create clear, accurate records of decisions and actions	Keep unnecessary drafts or duplicate information
Storing information	Save records in approved systems (SharePoint, Teams, business systems)	Store records in Outlook inboxes or local drives
Naming and version control	Use clear file names and SharePoint version history	Use vague names like "final", "latest", or save multiple copies
Protecting information	Apply Red/Amber/Green classification and restrict access	Share information with people who don't need it
Incident reporting	Report security incidents and potential data breaches immediately via IT Self Service and cooperate with investigations	Delay reporting or ignore incidents, even if unsure of severity
Sharing information	Check recipient details and use secure methods (Purview labels, Safedrop, secure post)	Send sensitive data via unsecured email or incorrect recipients
Phishing and cyber security	Be cautious of unexpected emails, links, and attachments; report suspicious messages	Click links or download software unless you trust the source and it's approved

1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page **62** of **63**

Devices and removeable media	Use encrypted devices and keep passwords separate	Store passwords with devices or connect personal devices to SCC equipment
Retention and disposal	Follow retention periods and dispose of information securely	Keep information “just in case”
Physical records	Store securely (locked cabinets/RMC) and track movement	Leave records unattended or in unsecured locations
Working remotely	Keep devices secure and be mindful in public spaces	Access sensitive (Red) information in public
Studying and training	Anonymise case studies and follow data protection requirements	Include identifiable personal or confidential information in assignments
When unsure	Ask your manager or Information Governance team and report issues	Ignore risks, mistakes, or potential data breaches

Remember: The more sensitive the information, the greater the care and protection required.

1. Suffolk County Council Records Management Handbook | Version 1.0
2. Approved by: Head of Information Governance | Owner: Information Governance team
3. Last reviewed: June 2026 | Next review due: June 2027
4. SCC internal use only | Page **63** of **63**