RECORDS MANAGEMENT POLICY

We will on request produce this Policy, or particular parts of it, in other languages and formats, in order that everyone can use and comment upon its content.

Owner: SIRO
Document ID: ICT-PL-0098
Version: 1.3
Date: March 2021
Review date: March 2023

DOCUMENT MANAGEMENT

Version	Date	Summary of Changes
1.0	May 2015	First version
1.1	November 2016	Review and Updates
1.2	December 2018	Review and Updates
1.3	March 2021	Review and updates

Accountable Owner		Approval date
Senior Information Risk Owner (SIRO)	Chris Bally	04/07/2021

Responsible Owner		Approval date
Head of Information Governance	Peter Knight	21/04/2021

Reviewers	Role	Approval date
Policies Review Group: Russell Armstrong Philip Barbrook Anna Stephenson (policy review lead) Joanne Withey Corporate Information Governance Board - ratification	 IT Security Manager Enterprise Architect DPO & Compliance Manager DP & Training Manager	18/05/2021 29/07/2021

Publication information		
	Published (if YES, enter document location)?	**Location**
All staff	Yes	SCC intranet - mySCC
Public	Yes	SCC website

1. Introduction

a) Suffolk County Council (SCC) recognises that its records are an important public and corporate asset, and are a key resource required for its effective operation and accountability. This policy sets out SCC's responsibilities in relation to records management.

b) This policy also includes the UK General Data Protection Regulation's (GDPR) data standards (i.e., data minimisation, data accuracy and storage limitation) which Services should apply to the management of records containing personal data. Each of the data standards together with guidance on how to apply them is set out in Appendices A, B and C of this policy.

Following this guidance supports SCC's technical and organisation measures to implement the data protection principles effectively and safeguard individuals' rights (this is known as 'data protection by design and by default').

c) This policy applies to the employees of SCC, SCC Councillors, any partners, voluntary groups, third parties and agents who SCC employees have authorised to access SCC information, including contractors and vendors. For the purposes of this policy all these individuals are referred to as 'users' and they are responsible for taking the steps outlined below whilst working with SCC information.

d) When reading this policy, you should be aware of, and where appropriate access, the following policies which are also relevant to good records management practices:

- Staff Acceptable Use of Information Systems
- Caldicott Principles
- Classification and Labelling of Information Policy
- Freedom of Information Policy
- Data Protection Policy
- Password Management Policy
- Specific Directorate/Service records management policies

e) For further information and advice about this policy, you should contact either your Directorate's Strategic Information Agent (SIA) or the Information Governance team (data.protection@suffolk.gov.uk).

2. Roles and responsibilities

SCC has a corporate responsibility to maintain its records and record-keeping systems in accordance with legislative requirements.

The following roles are responsible for ensuring compliance with this policy.

a) **SIRO**: this role is fulfilled by the Deputy Chief Executive and Director of Corporate Services who is the accountable owner of this policy.

b) **Head of Information Governance** is the responsible owner of this policy and co-ordinates record-keeping activities with the Records Manager and Data Protection Officer & Compliance Manager.

c) **Head of Suffolk Archives** is responsible for the permanent preservation of records.

d) **Directors**: are responsible for the management of their Services' records in compliance with this policy and for ensuring that all staff are aware of record keeping procedures. Dataset Owners (DSOs) are accountable to Directors for their operational ownership of the records and information contained in their systems.

e) **Managers** are responsible for supporting staff training and must raise non-completion of training with HR if any staff member does not or cannot complete the requisite training requirements.

   Staff with specific responsibilities for records management should have these duties clearly defined in their job descriptions.

f) **Dataset Owners (DSOs)**: are usually business managers who operationally own and are responsible for the information and records contained in their systems (paper and/or electronic).

   DSOs are required to understand what information and records are held within their Directorates' Services, how they are used (including how long they are needed for) and transferred, and who has access to them and why, so that business can be transacted within an acceptable level of risk. DSOs are recorded in the Council's Registers of Datasets.

g) **Dataset Managers (DSMs)**: are usually responsible for the daily management of information and records within their Service. Their responsibilities include the escalation of any potentially non-compliant records management activities to the relevant DSO. DSMs are recorded in the Council's Registers of Datasets.

h) **Strategic Information Agents (SIAs**): each Directorate's SIA(s) is responsible for ensuring that its Directorate's/Services' Register of Datasets is regularly reviewed and updated to include each dataset's retention period.

i) **Information Governance Leads (IGL)**: each Directorate's IGL is responsible for ensuring it Directorate is managing the retention and destruction of its records in line with its Directorate's/Services' retention periods.

j) **Monitoring Officer** is responsible for ensuring that adequate induction and training is undertaken by Councillors and that support is provided to them in relation to complying with this policy.

k) **Data Protection Officer** is responsible for addressing any records management queries raised directly with the Data Protection Officer by either SCC staff or the public.

l) **All users** are responsible for creating and maintaining accurate records in relation to their work. This policy should support all users to understand good records management practices.

3. Training and awareness

a) It is important that all users understand their records management responsibilities. Mandatory information governance training '*Keeping Information Safe:, Our Information, Our Responsibilities'* must be undertaken by all SCC staff, and it is mandatory for that training to be refreshed every two years.

b) The Information Governance team monitors the uptake of mandatory training and service managers are responsible for ensuring staff have access to this training.

c) Service managers are also responsible for ensuring staff receive bespoke training in relation to Directorate/Service specific records management practices.

4. Record creation, maintenance, and disposal

a) A record is any recorded information regardless of medium (including, but not limited to, paper, microform, electronic and audio-visual) which is created, collected, processed, used, stored and/or disposed of by SCC's staff, as well as those acting as its agents to undertake a Council activity.

b) The storage of records may include:

- IT systems/databases and electronic file paths
- Email
- Filing cabinet
- Shelves
- Personal storage space e.g. lockers
- Microsoft Teams groups
- Sharepoint collaborative work spaces
- Sharepoint One-drive
- Microsoft Outlook calendars
- Internal e.g. mySCC and external websites
- Records held at the Council's Records Management Centre

c) Directors, Managers, DSOs, and DSMs (see paragraph 2(d), (e), (f) and (g) above) within Services must ensure that all electronic and paper systems, which contain records, must be able to document activities and can provide quick and easy retrieval of information. Services must also consider the legal and regulatory context specific to their area of work.

d) Electronic and paper systems containing records must be maintained by Services to ensure that records are properly stored, protected, and can easily be located and retrieved. Information about online storage areas and what you should use them for is available from IT Services Where can I save my online files?.

e) Directorates/Services must have in place clearly defined arrangements for the review and selection of records for disposal which must be documented (see Appendix C).

f) Directorates/Services using the Records Management Centre to store records must ensure they are managed in line with the Centre's procedures. Each Directorate is responsible for ensuring it has procedures in place for the review and disposal or archiving of records deposited with the Centre.

5. Access and security

a) All SCC's records will be subject to appropriate security measures as set out in the Council's Information Security and Acceptable Use of Information Systems policies. Directors, Managers, DSOs, and DSMs must ensure that:

- all staff are aware of the arrangements for allowing access to certain types of information; and
- procedures are in place to document decisions concerning access;
- by default, users processing information for and on behalf of SCC should only have access to information that is relevant for the purposes of carrying out their duties.

b) It is the responsibility of all users to ensure that where the printing solution called FollowMe is available within SCC's premises, they print documents using the FollowMe option. FollowMe printing enables users to send documents to print and requires the user to swipe their ID cards at the printer before it will print.

c) Paper records containing sensitive information, or which are classified as 'Official Sensitive' must be destroyed using secure waste sacks or bins located in SCC's premises. If you are working from home, you should either shred the information using a cross-shredder or secure the information until you can dispose of it using SCC's secure disposal facilities.

d) Records held in electronic formats, e.g., encrypted memory stick, must be destroyed in line with guidance from IT Services. Queries should be made via the IT Helpdesk.

e) Transferring records which contain sensitive or 'Official Sensitive' information electronically must be sent to recipients securely. If you are unsure about secure electronic transfers, you should check the Acceptable Use of Information Systems policy. If you remain in doubt you should check with either your Manager or your Directorate's Strategic Information Agent (SIA).

f) Transferring paper records which contain sensitive data or information which is labelled 'Official Sensitive' must be sent to recipients securely. If you are unsure about the secure methods your service uses for transferring paper records you should check with your Manager or Directorate SIA.

6. Non-compliance with this Policy

a) Failure to comply with this policy may lead to further action and investigation under SCC's disciplinary procedures. In certain circumstances, non-compliance with this policy may be considered gross misconduct, and could result in dismissal.

b) It should be noted non-compliance with this policy could also lead to criminal or civil action if illegal activities are involved or legislation is contravened. SCC will not hesitate to bring to the attention of the appropriate authorities any use of its systems which it believes might be illegal.

c) Failure by County Councillors to comply with this policy may contravene the *Members' Code of Conduct* and could lead to a referral to the Council's Monitoring Officer (see paragraph 2(h) above).

d) **Security incidents**: all staff must report suspected security incidents via IT Self Service *'Report an Incident'* within 24 hours of being made aware of them.

APPENDIX A

Data Minimisation

1. One element of compliance with the Accountability principle under the UK GDPR is to ensure that SCC is only collecting and holding the data it needs to about individuals. Personal data must not be collected on the off chance that it might be useful in the future.

2. If SCC's Services are holding more data than is necessary for their purposes, this is likely to be unlawful (most of the lawful bases for processing have a necessity element) as well as a breach of the Data Minimisation principle. It also means that individuals will have the right to erasure (also known as the right to be forgotten).

3. To support compliance with the Accountability principle, Services should identify the minimum amount of personal data that is needed to fulfil their purposes. They should only hold that much information, and no more, which means Services must ensure that the data they are processing is:

    - Adequate i.e., sufficient to properly fulfil the stated purpose;
    - Relevant i.e., has a rational link to that purpose e.g., it is not being included in a record because it 'may be useful'.
    - limited to what is necessary i.e., the Service is not holding more information than it needs for that purpose.

4. To assess whether a Service is holding the right amount of personal data, it must be clear about why it needs it and take the following points into account:

    a) For special category data or criminal offence data, it is important to make sure only the minimum amount of information is collected and retained. This means a Service may need to consider this element separately for each individual, or for each group of individuals sharing relevant characteristics.

    b) Services should also consider any specific factors that an individual brings to its attention e.g., as part of an objection, request for rectification of incomplete data, or request for erasure of unnecessary data.

    c) Services should periodically review their processing to check that the personal data they hold is still relevant and adequate for their purposes and delete anything that is no longer needed. This is closely linked with the storage limitation principle (see Appendix C).

    d) Services are likely to be processing too much personal data if they are not regularly reviewing the collection of data in line with their purposes, reviewing datasets at the end of their retention period, and destroying data when it is no longer needed.

5. Where services are holding data about individuals that constitute a record of an opinion, this data is not necessarily inadequate or irrelevant personal data, just because that individual disagrees with or thinks it has not considered information they

think is important. The following factors should be considered when recording opinions:

a) For the information to be adequate (see paragraph (1) above), an individual's records should make it clear that it is an opinion rather than fact. The record of the opinion (or of the context it is held in) should also contain enough information to enable a reader to interpret it correctly. For example, it should state the date and the author's name and position.

b) If an opinion is likely to be controversial or very sensitive, or if it will have a significant impact when used or disclosed, it is even more important to state the circumstances or the evidence it is based on. If a record contains an opinion that summarises more detailed records held elsewhere, the Service should make this clear.

APPENDIX B

Data Accuracy

1. Where Services use their own resources to compile personal data about an individual, they must ensure the information recorded in the individual's record is correct. Failure to ensure the accuracy of individuals' data could have serious implications for an individual and could lead to a security incident.

2. It may be impractical to check the accuracy of personal data someone else provides. Where this happens, Services should:

    - accurately record the information provided;
    - accurately record the source of the information;
    - take reasonable steps in the circumstances to ensure the accuracy of the information; and
    - carefully consider any challenges to the accuracy of the information.

3. Reasonable steps will depend on the circumstances and the nature of the personal data and what a Service is using it for. The more important it is that the personal data is accurate, the greater the effort the Service should put into ensuring its accuracy.

4. If a Service has taken all reasonable steps to ensure the accuracy of an individual's data, and subsequently receives information which suggests it may be wrong or misleading, the Service needs to urgently reconsider whether it is accurate and take steps to erase, update or correct it in light of the new information.

5. The GDPR provides individuals with the following rights to challenge data inaccuracies, they are:

    a) The right to challenge the accuracy of personal data (this is known as the right to rectification). If this happens, the Service should consider whether the information is accurate and, if it is not, the Service must delete or correct it. It is important to note that individuals have the absolute right to have incorrect personal data rectified.

    b) The right to erasure (this is also known as the right to be forgotten). Individuals do not have the right to erasure just because data is inaccurate. However, the GDPR's accuracy principle require SCC to take all reasonable steps to erase or rectify inaccurate data without delay, and it may be reasonable to erase the data in some cases. If an individual asks you to delete inaccurate data, it is therefore good practice to consider this request.

    The procedure for managing these requests is available from the mySCC Information Governance pages.

APPENDIX C

Retention of Personal Data (Storage Limitation) Guidance and Checklist

1. Introduction

a) Under the UK General Data Protection Regulation's (GDPR) Storage Limitation principle, SCC must not keep the personal data it is collecting and processing for longer than is needed.

b) Managing the retention of records is important for the following reasons:

i. Ensuring Directorates and their Services erase or anonymise personal data when it is no longer needed, will reduce the risk that it becomes irrelevant, excessive, inaccurate, or out of date. This also reduces the risk that the Service will use such data in error which could cause a security incident.

ii. If personal data is held for too long it will, by definition, be unnecessary, and the lawful basis for processing is unlikely to apply to the retention of that data.

iii. From a practical perspective, it is inefficient to hold more personal data than is needed, and there may be unnecessary costs associated with storage and security.

iv. Directorates and their Services may need to respond to subject access requests for any personal data they hold. It may be difficult to provide full responses if Directorates and their Services are holding data for longer than they need to.

v. If Directorates and their Services employ good practice around storage limitation, for example they have thought about, and are able to justify, how long they hold personal data for, the retention periods have been recorded in the appropriate Register of Datasets, and the destruction of data is effected at the appropriate time, these practices are likely to reduce the burden of dealing with queries about retention and individuals' requests for erasure.

c) The GDPR does not set specific time limits for retaining different types of data and within the context of SCC, it is up to each Directorate and its Services to decide how long it should retain data for, which will depend on how long it needs the information for its specified purposes.

2. How to set retention periods

The GDPR does not stipulate how long organisations should keep personal data. Consequently, it is up to each Directorate and its Services within SCC to justify this, based on its purposes for processing. Retention of personal data must always be fair

and lawful, and Directorates and their Services should take a proportionate approach, balancing their requirements with the impact of retention on individuals' privacy.

Each Directorate and its Services is in the best position to determine how long it needs to retain data. The following factors should assist Services with setting retention periods.

a) Services must be able to justify why it needs to keep personal data in a form that permits identification of individuals. If the Service does not need to identify individuals, it should anonymise the data so that identification is no longer possible.

b) Services should consider their stated purpose for processing the personal data (this can be found in each Directorate's Register of Datasets). Services can retain data for as long as the purpose (of if there are more than one, the purposes) still applies. Services should not, however, keep data indefinitely i.e., 'just in case'.

c) Where Services are collecting and recording information about individuals, they should consider whether they need to retain all the information that is held about them once the relationship with the Service ends. This is known as data minimisation (see Appendix A).

d) Services should consider whether they need to keep information to defend possible future legal claims. If it is decided that data needs to be kept for this purpose, the Service must consider deleting personal information that could not possibly be relevant to such a claim. In addition, unless there is some other reason for keeping it, personal data should be deleted when such a claim could no longer arise.

e) Services should consider any legal or regulatory requirements. There are various legal requirements and professional guidelines about keeping certain kinds of records – such as information needed for income tax and audit purposes, or information on aspects of health and safety and health and care purposes. Services who retain personal data to comply with a requirement like this, will not be considered to have kept the information for longer than necessary.

f) Services should consider any relevant industry standards or guidelines. These could be a good starting point for setting standard retention periods and are likely to take a considered approach, but bear in mind, they do not guarantee compliance. Services must still be able to explain why retention periods are justified.

g) Services may be able to hold information for a foreseeable event that may never occur provided they can justify it, for example future legal claims, safeguarding concerns, investigatory purposes. Where a Service believes it can justify holding data in this instance, they should discuss this with their Director and the dataset's DSO. The Data Protection Officer should also be consulted in the event of uncertainty in this respect. Services should ensure the justification for keeping data for potential foreseeable events is recorded.

h) Personal data may be retained indefinitely if Services are holding it for **archiving, research, or statistical purposes**, and one of the following reasons are met:

- archiving purposes in the public interest
- scientific or historical research purposes; or
- statistical purposes.

If a Service can justify retaining personal data for one of the above purposes, it must have appropriate safeguards in place to protect individuals, for example, pseudonymisation may be appropriate in some cases.

The purpose for retention must be the Service's only purpose and it cannot later use that data for another purpose - in particular for any decisions affecting particular individuals. **Note**: this does not prevent other organisations from accessing public archives, but they must ensure their own collection and use of the personal data complies with the principles.

3. **When to review your retention periods**

a) Services should review whether they still need personal data at the end of any standard retention period, and erase or anonymise it unless there is a clear justification for keeping it for longer. Automated systems can flag records for review or delete information after a pre-determined period. This is particularly useful if the Service holds many records of the same type.

b) It is also good practice for Services to review retention periods for personal data at regular intervals prior to the end of the retention period, especially if the standard retention period is lengthy or there is potential for a significant impact on individuals.

c) If Services have not set retention periods for the personal data they process, they must regularly review whether they still need it, and evidence that those reviews have been undertaken.

d) Services must also be prepared to review whether they still need personal data if an individual asks them to. Individuals have the absolute right to erasure of personal data that a Service no longer needs for its specified purposes, see Appendix B, paragraph (5) above).

e) Personal data that has been pseudonymised – e.g., key-coded – will usually still permit identification. Pseudonymisation can be a useful tool for compliance with other principles such as data minimisation (see Appendix A) and security, but the storage limitation principle still applies.

4. **Where to record your retention periods**

a) In compliance with the GDPR, SCC is required to keep a record of all its personal data processing activities. SCC's processing activities are recorded in its Registers of Datasets. Each Directorate is assigned its own Register and must, amongst other requisite information, record its retention period for each dataset.

b) The Registers are maintained by each Directorate's Strategic Information Agent. Every two years each Directorate is required to undertake a formal review of its dataset entries. The reviews are co-ordinated by the Information Governance team.

c) Services should ensure their Directorate's/Service's privacy notices include information about its retention periods and update them as and when there are changes. Every two years each Directorate is required to undertake a formal review of its Directorate's/Services' Privacy Notices. The reviews are co-ordinated by the Information Governance team.

5. Information sharing

a) If Directorates and their Services share personal data with other organisations or contractors, they must undertake a Data Protection Impact Assessment in relation to completing either an Information Sharing Agreement (ISA) or a Data Processing Schedule (DPS) for inclusion in a contract.

b) ISAs and DPSs include arrangements agreed between the Service and the organisation/its contractor for managing shared information. For example, under an information sharing agreement, a Service may agree to return the shared data to the organisation that supplied it without keeping a copy. In other cases, the Service may decide that its contractor should delete its copies of the personal data and confirm in writing that this action has been completed.