Data Protection 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.

Document ID: ICT-PL-0099
Version: 1.6
Date: December 2025
Review date: December 2027

DOCUMENT MANAGEMENT

Version	**Date**	**Summary of Changes**
1.0	January 2010	First version
1.1	May 2015	Review and updates
1.2	December 2017	Review and updates
1.3	May 2018	Review and updates
1.4	March 2021	Review and updates
1.5	June 2023	Review and updates
1.6	November 2025	Review and updates

Accountable Owner		**Approval date**
Head of Information Governance	Peter Knight	04/12/2025
Head of Information Governance	Peter Knight	19/07/2023

Responsible Owner		**Approval date**
DPO + Compliance Manager	Anna Stephenson	05/11/2025
DPO + Compliance Manager	Anna Stephenson	04/12/2023

Reviewers	**Role**	**Approval date**
Policies Review Group: John Thurkettle Peter Knight Anna Stephenson Joanne Withey	 IT Security Manager Head of Information Governance DPO & Compliance Manager DP & Training Manager	(see above)
Nigel Inniss	SIRO	
Corporate Information Governance Board (CIGB)		

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

1. INTRODUCTION

a) To operate efficiently, Suffolk County Council (SCC) must collect and use information about people with whom it works. This may include members of the public, service users, current, past, and prospective employees, clients, customers, contractors, suppliers, and partner organisations. In addition, some laws may require SCC to collect and use information to comply with the requirements of central government.

b) SCC regards the lawful and correct treatment of personal information as critical to its successful operations, maintaining confidence between SCC and those with whom it carries out business. SCC will ensure that it manages personal information in compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Data (Use and Access) Act 2025 (collectively referred to as data protection law).

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

d) Linked/Other useful policies include:

- Acceptable Use of Information and Systems
- Artificial Intelligence (AI)
- Freedom of Information
- Information Security Incident Reporting and Management
- Password Management
- Records Management
- Social Media
- Appropriate Policy Document for Processing Special Category and Law Enforcement Personal Data Processing
- Surveillance Camera

2. SCOPE

a) This policy does not apply to requests for access to adoption records, which should be referred to the Adoption and Fostering Service.

b) This policy does not apply to information held by schools. If a request concerns data protection in a school or a wish to access school records, the requester should contact the Headteacher of the relevant school.

c) Elected Members (Councillors) should note that they are also data controllers and are responsible for ensuring any personal information they hold/use in their office as elected Members is handled in accordance with data protection law.

d) Data protection law does not apply to requests for information about a person if they are deceased. These requests should be processed in accordance with the Freedom of Information Act (FOIA) 2000 but should also be considered fairly and lawfully.

e) SCC will have a person in the role of Senior Information Risk Owner (SIRO), who will have oversight of all information risks including those relating to personal data. The SIRO will take all appropriate actions at Corporate Leadership Team (CLT) level to ensure that such risks are understood and managed effectively. The SIRO will also be the corporate champion for data protection and will also ensure that the organisation obtains the benefits from sharing personal data lawfully and fairly within SCC and beyond. The SIRO role is undertaken within SCC by the Assistant Director of Governance, Legal and Assurance.

f) SCC will appoint a Data Protection Officer (DPO) who will advise on compliance with the law and areas such as privacy by design and liaise with the ICO as required. The Data Protection Officer role is undertaken within SCC by the Council's Data Protection Officer and Compliance Manager.

g) SCC will have a Corporate Information Governance Board (CIGB) that will promote, maintain, and review information management and risk, make relevant decisions, and will make recommendations to CLT where appropriate.

3. STAFF RESPONSIBILITIES

a) This policy applies to all employees, elected Members (Councillors), contractors, agents, representatives, and temporary staff, working for or on behalf of SCC.

b) This policy applies to all personal information created or held by SCC, in whatever format. This includes, but is not limited to, paper, electronic, email, microfiche, and film.

c) The Head of Information Governance is accountable for ensuring compliance with this policy.

d) The DPO will assist with the monitoring of internal compliance, inform, and advise the Council of its data protection obligations, provide advice regarding information risk assessment, and act as a contact point for data

subjects and the Information Commissioner's Office (ICO).

e) The Information Governance team is responsible for providing day-to-day advice and guidance to support the Council in complying with this policy**.**

f) SCC Directors are responsible for ensuring that business areas they have responsibility for have processes and procedures in place that comply with this policy. They are responsible for ensuring that data is appropriately protected or that controls are in place to prevent access by unauthorised personnel, and that data cannot be tampered with, lost or damaged.

g) Strategic Information Agents (SIAs) are responsible for promoting openness and accountability in their service area. Each SIA will promote good practice and assist their Directorates in ensuring compliance with this policy. The nomination of such a person shall not release other members of staff from compliance with this policy.

h) Dataset Owners are responsible for ensuring that the information contained within their systems (paper or electronic) is stored, processed, and transferred in accordance with this policy.

i) SCC appoints Caldicott Guardians to provide advice to ensure that where health related personal information is shared (particularly in relation to patients, children, and vulnerable adults) it is done properly, legally, and ethically:

- Adult Social Care - Head of Business Management
- Children and Young People's Services - Head of Safeguarding
- Public Health - Assistant Director of Public Health

j) All members of staff, contractors and elected Members who hold or collect personal data are responsible for their own compliance with data protection law and must ensure that personal and/or sensitive information is kept and processed in accordance with this policy. Staff must not attempt to access personal data that they are not authorised to view. Failure to comply with this policy may result in disciplinary action which could further lead to dismissal and, in some cases, criminal proceedings/prosecution.

k) All members of staff are responsible for keeping up to date with any guidance and/or communications which may be circulated via internal newsletters (e.g. InsideSCC), the intranet (e.g. the Information Governance pages), or other bulletins.

4. TRAINING

a) All members of staff are required to undertake mandatory data protection training every 12 months. The Information Governance team is responsible for the roll-

out of mandatory and refresher data protection training.

b) Managers are responsible for ensuring that adequate induction and mandatory training is undertaken by staff. Line managers have a responsibility to support this training and must raise this matter with HR if any staff member does not or cannot complete the training.

c) Managers are responsible for ensuring that staff undertake any additional relevant training in relation to their specific roles and access to relevant systems.

d) The Monitoring Officer is responsible for ensuring that adequate induction and training is undertaken by Councillors and that support is provided to them so as to implement this policy. All Councillors are required to undertake mandatory information governance training following an election.

5. GOVERNANCE

a) SCC's Corporate Information Governance Board (CIGB), SIRO and DPO will ensure compliance with data protection law and this policy.

b) SCC will have continuous improvement mechanisms, audits, compliance plans, and inspections to ensure compliance with data protection law and this policy.

6. PRIVACY BY DESIGN

a) Data protection law, requires:

- **data protection by design:** data controllers must put technical and organisational measures such as pseudonymisation in place – to minimise personal data processing; and
- **data protection by default:** data controllers must only process data that are necessary for the purposes of processing and must only store data as long as it is necessary to do so.

b) SCC will have the appropriate measures in place to determine the basis for lawful processing and will undertake information risk assessments to ensure compliance with the law. These measures will include the use of Data Protection Impact Assessments (DPIAs) and other processes as agreed with the DPO.

c) SCC uses an information classification scheme (see Appendix A) to identify the sensitivity of its information for the purposes of assessing and minimising risks associated with the processing of data.

7. CONTRACTS

a) Data protection law places significant requirements on both SCC and its

suppliers to ensure the security of personal data, and to manage individuals' privacy rights. This means whenever SCC uses a supplier to process individuals' data on its behalf it must have a written contract in place.

b) Under data protection law the parties to a contract need to understand their responsibilities and liabilities in relation to the data within scope of their contracts.

c) SCC is liable for its compliance with data protection law and must only appoint suppliers who can provide 'sufficient guarantees' that the requirements of the law will be met, and the rights of individuals protected.

d) If a contractor, partner organisation or agent of SCC is appointed or engaged to collect, hold, process, or deal with personal data on behalf of the council, or if the contractor will do so as part of the services they provide to SCC, the relevant lead Council officer must ensure that personal data is managed in accordance with data protection law and this policy.

e) Security and data protection requirements must be included in any contract that the agent, contractor, or partner organisation enters into with SCC and reviewed during the contract's lifecycle.

f) SCC staff will use the appropriate processes, templates, and Data Protection Impact Assessments (DPIAs) when managing and/or issuing contacts.

8. INFORMATION SHARING

a) Data protection law does not prevent SCC from sharing information when it is in the best interests of the data subject and when failure to share data may carry risks to vulnerable groups and individuals.

b) Information must always be shared in a secure and appropriate manner and in accordance with its information type and classification.

c) SCC will be transparent and as open as possible about how and with whom data is shared; with what authority; for what purpose; and with what protections and safeguards.

d) All information sharing should be included in Directorate/Service privacy notices and reviewed on a regular basis.

e) SCC's Information Sharing Agreements (ISAs) are recorded in the corporate Register of DPIAs which is available to SCC staff. All SCC generated ISAs must be supported by a DPIA. SCC staff should contact the Information Governance team if they have any queries about completing a DPIA for information sharing purposes. Dataset Owners are responsible for the implementation and management of ISAs.

9. INDIVIDUALS' RIGHTS

a) An individual may request a copy of any data held about them, or information about the reasons for which it is kept and processed. This is called a Subject Access Request (SAR). Information on how an individual can make a SAR can be found on the Council's external web pages under Privacy and Data Protection.

b) Individuals also have other rights under data protection law which are set out in the corporate privacy notice. SCC must respond to individuals exercising their rights within one month.

c) Under data protection law, individuals can submit complaints about SCC's handling of their personal data via either the corporate complaints process or directly to the Information Governance team. Complaints must be acknowledged within 30 days of receipt and responded to without undue delay. It is recommended that responses to complaints are provided within 30 days from the date of acknowledgement.

d) National Data Opt-Out: SCC reviews all of its data processing on an annual basis to assess if the national data opt-out applies, which, if it does apply, is recorded in the relevant Directorate's Register of Datasets. All new processing is assessed to see if the national data opt-out applies. If any data processing falls within scope of the National Data Opt-Out, SCC uses MESH to check if any of our service users have opted out of their data being used for this purpose.

10. DISCLOSURE OF PERSONAL INFORMATION

a) Personal data must only be disclosed in accordance with data protection law.

b) All staff, contractors and individuals working for or on behalf of SCC must ensure they are satisfied as to the identity of a requestor before disclosing personal data. They should also ensure that the requestor is, in line with data protection law, entitled to access the information requested.

c) When disclosing personal data, all staff, contractors and individuals working for or on behalf of SCC must ensure only the minimum amount of data is disclosed for the requested purpose.

11. DATA QUALITY, INTEGRITY AND RETENTION

a) The Information Governance team must be contacted should any issues or complaints be raised by data subjects about personal data quality and/or integrity.

b) SCC holds information, whether electronic or paper, in line with our Records

Management Policy and the Registers of Datasets.

c) SCC's records retention information is included in the Registers of Datasets.

12. SURVEILLANCE CAMERAS

a) Surveillance camera monitoring must only be carried out in accordance with the Surveillance Camera Code of Practice (March 2022), issued under the Protection of Freedoms Act (PoFA) 2012 and the ICO's Guidance on Video Surveillance (including CCTV). For more information, see SCC's Surveillance Camera policy.

b) The covert surveillance activities of the law enforcement community are not covered here because they are governed by the Regulation of Investigatory Powers Act (RIPA) 2000, Investigatory Powers Act 2016 and Regulation of Investigatory Powers (Scotland) Act (RIPSA) 2000.

c) The use of conventional cameras (not CCTV) by the news media or for artistic purposes such as for film making are not covered by this policy because they are subject to special treatment under data protection law. However, this policy does apply to the passing on of CCTV images to the media.

13. DATA ETHICS

The Council has published its Ethical Data Stewardship Charter to demonstrate the Council's commitment to a set of principles which govern the use of data. The Charter outlines the processes to be followed for ethical risk assessment and decision-making and includes the following principles:

1. Accountability
2. Scrutiny
3. Transparency
4. Participation
5. Design
6. Oversight
7. Fairness
8. Benefit

The full Charter is available on the Council's website Ethical-Data-Stewardship-Charter.pdf (suffolk.gov.uk).

SCC's Ethics Advisor (the role is currently held by the DPO & Compliance Manager (DPO)) is responsible for referring data ethics matters to and convening meetings of the Data Ethics Advisory Panel.

14. SECURITY INCIDENTS

All suspected breaches of information security must be reported within 24 hours of their discovery via IT Self Service using the *Information Security Incident report form*.

15. NON-COMPLIANCE WITH THIS POLICY

a) Non-compliance with this policy may result in employees being subject to disciplinary action under SCC's Disciplinary and Capability Policies. Non-compliance by Councillors may be in breach of the *Members' Code of Conduct* and may lead to a referral to the Council's Monitoring Officer.

b) In certain circumstances, the non-compliance of employees with this policy may be considered gross misconduct resulting in dismissal. It should be noted that non-compliance with this policy could also lead to criminal or civil action if illegal material is 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.

APPENDIX A – INFORMATION CLASSIFICATION SCHEME

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