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: 1.5
Date: June 2023
Review date: June 2025

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

Accountable Owner		Approval date
Head of Information Governance	Peter Knight	19/07/2023
Senior Information Risk Owner	Chris Bally	05/07/2021

Responsible Owner		Approval date
DPO & Compliance Manager	Anna Stephenson	30/06/2023
Head of Information Governance	Peter Knight	21/04/2021

Reviewers	Role	Approval date
Policies Review Group: John Thurkettle Anna Stephenson (Policy review lead) Joanne Withey Peter Knight Corporate Information Governance Board	 IT Security Manager DPO & Compliance Manager DP & Training Manager Head of Information Governance	22/06/2023

Publication information		
	Published (if YES, enter document location)?	**Location**
All staff	Yes	SCC 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), and the Data Protection Act 2018 (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 Systems
- Information Classification & Labelling
- 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 Director of Corporate Services/Deputy Chief Executive.

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 and Community Services - 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.

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, at least once every two years. 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.

c) Where anyone in SCC intends to process personal data relating to law enforcement, criminal or national security data they must seek advice from the Data Protection Officer before proceeding.

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 Assessment (DPIAs) and other processes as agreed with the DPO.

c) SCC uses its Information Classification and Labelling policy to assess information risks and includes special category 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) The law sets out what needs to be included in the contract so that both parties understand their responsibilities and liabilities.

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. 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.

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

8. INFORMATION SHARING

a) SCC may share 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 the 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; and for what purpose; and with what protections and safeguards.

d) SCC's Information Sharing Agreements (ISAs) are published in a corporate ISA Register. The Information Sharing Assurance Framework (ISAF) sets out SCC's requirements for compliance with data protection law and this policy. These documents can be found on the Data Protection pages of SCC's intranet (mySCC).

e) When information is shared with other organisations or partners, a formal ISA must be in place that is signed by all parties. Responsibility for its implementation lies with the Dataset Owner. The ISAF provides guidance for

completing ISAs and can be found on the Data Protection pages of mySCC.

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) The UK GDPR is specific about the information SCC needs to provide to people about what it does with their personal data and is published in documents called privacy notices. Guidance about privacy notices can be found on the Data Protection pages of mySCC.

d) SCC's privacy notice can be found on SCC's external website. The notice provides an overview about how SCC collects and uses people's data.

e) In addition to the corporate privacy notice, directorates, in compliance with data protection law must provide privacy notices. These notices can also be found on SCC's external website.

f) 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 ABOUT THIRD PARTIES

a) Personal data can only be disclosed about a third party in accordance with data protection law.

b) If a user believes it is necessary to disclose information about a third party to a person requesting data, they must seek advice from the Data Protection Team within the Information Governance team.

c) All contractors and individuals working for or on behalf of SCC must ensure identity checks are undertaken before providing personal data over the telephone.

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 forms part of the Register 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 the 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

In 2021, the Council developed and published an Ethical Data Stewardship Charter to demonstrate the Council's commitment to a set of principles which govern the use of data, and outlines the processes to be followed for ethical risk assessment and decision-making. The eight principles of the Charter are:

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).

In 2023/24, the Council will be establishing a Data Ethics Advisory Panel, under the auspices of the Council's Audit Committee, which will operate in an advisory capacity to the Council, and will seek to ensure that the eight principles of the EDSC are upheld and will help to maintain public trust.

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. COMPLAINTS

Complaints about SCC's compliance with data protection law and responses to subject access requests are dealt with by internal review processes. Complaints should be put in writing and sent data.protection@suffolk.gov.uk.

15. 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*.

16. 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* ad 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.