Data Protection Policy

Owner	**: Head of Performance and Information Management**
Document ID	**: ICT-PL-0099**
Version	**: 4.0**
Date	**: May 2018**

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.

Contents

DOCUMENT CONTROL

Changes History

Issue No	Date	Amended By	Summary of Changes
1.0	January 2010	Chief Information Officer	Version 1.0
2.0	May 2015	Neal Scarff, Philip Barbrook, Adele Rhodes Girling, Duncan Farley	Review and Updates
2.1	December 2017	Adele Rhodes Girling	Minor changes for title and department changes
3.0	April 2017	Adele Rhodes Girling	GDPR compliance
4.0	May 2018	Anna Stephenson	GDPR

Authorisation (Responsible Owner)

Role	Name	Approval Date
Head of Performance and Information Management	Peter Knight	22/05/18

Approval (Accountable Owner)

Role	Name	Approval Date
Senior Information Risk Owner	Chris Bally	22/05/2018

Reviewers (Consulted)

Role & Review Responsibilities	Name	Approval Date
Data Protection Manager	Anna Stephenson	22/05/18
Head of Performance and Information Management	Peter Knight	22/05/18
Information Management and Cyber Security Specialist	Daniel Beaumont	22/05/18
Enterprise Architect	Philip Barbrook	22/05/18
Strategic Information Agents	Various	22/05/18

Distribution List - Once authorised (Informed)

Name	Organisation
All Users	See Section 1.2.1 of Policy

Review Period

Date Document to be Reviewed	By whom
April 2020	Information Policy and Compliance Manager

1 INTRODUCTION

1.1 Purpose

1.1.1 The purpose of this document is to state the Data Protection policy for Suffolk County Council (SCC) and its compliance in line with the General Data Protection Regulation (GDPR), and subsequent revised UK Data Protection law.

1.2 Scope

1.2.1 It is applicable 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.

1.3 Linked/Other useful policies/procedures

1.3.1 This policy should be read in conjunction with the:

- Acceptable Use of ICT Policy
- Caldicott Principles
- Classification and Labelling of Information Policy
- Freedom of Information Policy
- Data Quality Policy
- E-mail Acceptable Use Policy
- Information Security Incident Reporting and Management Policy
- Password Policy
- Records Management & Information Handling Policy; and
- Social Media policy

2 RESPONSIBILITIES

2.1 Suffolk County Council

2.1.1 **Training** - SCC will train users with regard to this policy.

Training for Councillors will be provided as part of the Councillors' Learning and Development Programme.

2.2 Performance and Information Management Team

2.2.1 **Implementation and Monitoring of Policy** – The Performance and Information Management Team is tasked with implementing this policy and monitoring its effectiveness.

2.3 **Managers**

2.3.1 **Induction, Training and Support** - Managers are responsible for ensuring that adequate induction and training is undertaken by staff and that support is provided to them so as to implement this policy (see 2.4.1).

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.

2.4 **Users**

2.4.1 **User Awareness and Training** - All users should attend appropriate training courses. SCC delivers modular training to all users who have access to the Council's data and network. These training modules inform users of the requirements of its ICT Security Policies. All users must engage with this training and complete all mandatory modules. 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.

2.4.2 **Breach of this Policy** - Staff found to be in breach of this policy may be disciplined in accordance with the Conduct and Capability Policy. In certain circumstances, breach of this policy may be considered gross misconduct resulting in dismissal. It should be noted that breach of the 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.

Councillors found to be in breach of this policy may be deemed to have breached the *Members' Code of Conduct* and this may lead to a referral to the Council's Monitoring Officer.

2.4.3 **Breach of Information Security** - Users must report all suspected breaches of information security using the Information Security Incident report form via IT Self Service.

3 EXECUTIVE SUMMARY AND RESPONSIBILITIES

3.1 To operate efficiently, SCC must collect and use information about people with whom it works. These 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.

3.2 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 treats personal information correctly in accordance with the law.

3.3 This policy does not apply to requests for access to adoption records, which should be referred to the Adoption and Fostering Service on: 01473 264800.

3.4 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 Head Teacher of the relevant school.

3.5 Elected Members 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.

3.6 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.

3.7 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 Management Team (CMT) 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.

3.8 In accordance with data protection law, 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 Information Commissioner's Office (ICO) as required. The Data Protection Officer role is undertaken within SCC by the Council's Data Protection Manager.

3.9 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 CMT where appropriate.

4 STAFF RESPONSIBILITIES

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

4.2 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.

4.3 The Director of Corporate Services & Deputy Chief Executive is accountable for ensuring compliance with this policy. The day-to-day responsibilities are delegated to the Head of Performance and Information Management.

4.4 The Data Protection Manager will undertake information audits and manage the information collected by the council, the issuing of privacy statements, dealing with requests and complaints raised and the safe disposal of information.

4.5 The Data Protection team within the Performance and Information Management team, is responsible for providing day-to-day advice and guidance to support the Council in complying with this policy**.**

4.6 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.

4.7 Strategic Information Agents (SIAs) are responsible for promoting openness and accountability in their service area.

4.8 Each SIA shall 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.

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

4.10 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

4.11 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 (see paragraph 2.4.2 above).

5 GOVERNANCE

5.1 SCC will have a Corporate Information Governance Board (CIGB), a Senior Information Risk Owner (SIRO) and a Data Protection Officer (DPO - see paragraph 3.8 above) to ensure compliance with data protection law and this policy.

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

5.3 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 Manager before proceeding.

6 PRIVACY BY DESIGN

6.1 The General Data Protection Regulation (GDPR), and subsequent revised UK Data Protection laws, require:

- **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.

6.2 SCC will have the appropriate measures in place to determine the basis for lawful processing and will undertake 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 Data Protection Manager.

6.3 SCC uses its Information Classification and Labelling policy to assess information risks and includes special category data

7 CONTRACTS

7.1 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.

7.2 The law sets out what needs to be included in the contract so that both parties understand their responsibilities and liabilities.

7.3 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.

7.4 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 they

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.

7.5 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.

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

8 INFORMATION SHARING

8.1 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.

8.2 Information must always be shared in a secure and appropriate manner and in accordance with the information type and classification.

8.3 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.

8.4 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).

8.5 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 Information Asset Owner. The ISAF provides guidance for completing ISAs and can be found on the Data Protection pages of mySCC.

9 INDIVIDUALS' RIGHTS

9.1 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.

9.2 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.

9.3 The 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.

9.4 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.

9.5 In addition to the corporate privacy notice, directorates, in compliance with data protection law must provide privacy notices.

10 DISCLOSURE OF PERSONAL INFORMATION ABOUT THIRD PARTIES

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

10.2 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 Performance and Information Management team.

10.3 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

11.1 The Data Protection Team must be contacted should any issues or complaints be raised around personal data quality and/or integrity.

11.2 SCC holds information, whether electronic or paper, in line with our Records Management & Information Handling policy and Information Asset Register.

11.3 SCC's records retention information is part of the Information Asset Register.

12 CCTV MONITORING

12.1 CCTV monitoring must only be carried out in accordance with the ICO's code of practice on CCTV.

12.2 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.

12.3 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 code as they are subject to special treatment under data protection law. However, this code does apply to the passing on of CCTV images to the media.

13 COMPLAINTS

13.1 Complaints about SCC's compliance with data protection law and responses to subject access requests are dealt with by internal review processes.

13.2 Complaints must be put in writing and sent to the Data Protection Manager, Performance and Information Management team.

14 BREACH OF POLICY

14.1 Any breach of this policy should be investigated in accordance with the mandatory procedures specified in the Information Security Incident Reporting and Management Policy.

14.2 SCC will always treat any data breach as a serious issue, potentially warranting a disciplinary investigation.

14.3 Each incident will be investigated and judged on its individual circumstances, addressed accordingly and carried out in line with the employee code of conduct.

15 REVIEW OF THE POLICY

15.1 This policy will be reviewed every two years or when any other significant change impacts upon the policy. Comments on the policy, from both employees and members of the public, are therefore welcome and can be addressed to:

Data Protection Manager
Performance and Information Management
Suffolk County Council
Constantine House
Constantine Road
Ipswich
Suffolk
IP1 2DH

data.protection@suffolk.gov.uk

16 FURTHER ADVICE

For further advice on this policy, please contact:

Your Strategic Information Agent, or the Data Protection Team