Data Protection Policy

Owner : **Head of Information Management**

Document ID : **ICT-PL-0099**
Version : **2.0**
Date : **May 2015**

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.

Table of 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, Duncan Farley	Review and Updates

Authorisation (Responsible Owner)

Role	Name	Approval Date
Head of Information Management	**Duncan Farley**	**15/05/2015**

Approval (Accountable Owner)

Role	Name	Approval Date
Senior Information Risk Owner	**Chris Bally**	**19/05/2015**

Reviewers (Consulted)

Role & Review Responsibilities	Name	Approval Date
Enterprise Architect	**Philip Barbrook**	**14/05/2015**
Policy & Compliance Manager	**Philip Barbrook**	**14/05/2015**
Information Management Operations Manager	**Adele Girling**	**14/05/2015**

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
May 2017	**Head of Information Management**

1 INTRODUCTION

1.1 Purpose

1.1.1 The purpose of this document is to state the Data Protection policy of Suffolk County Council (SCC).

1.2 Scope

1.2.1 It is applicable to SCC Councillors, the employees of SCC, 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 ‘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;
- Freedom of Information Policy;
- Data Quality Policy;
- E-mail Acceptable Use Policy;
- Protective Marking Policy;
- Records Management & Information Handling Policy;
- Password Management 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 CIO Information Management Team

2.2.1 **Implementation and Monitoring of Policy** – The CIO Information Management Team has been tasked to implement this policy and monitor 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 the 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 the 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 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. The Council 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 be a breach of the *Members' Code of Conduct* leading to action by the Standards Committee.

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

3.1 This policy outlines the principles of the Data Protection Act 1998 (DPA) and identifies how the Council will comply with that Act.

3.2 Designated personnel and their responsibilities are identified.

3.3 Specific details on how personal information will be processed are covered including:

- recording what personal information is processed;
- providing adequate security for personal information;
- identifying sensitive and high risk personal information;

- sharing personal information;
- monitoring; and
- disposing of personal information.

3.4 Procedures on accessing and disclosing personal information to individuals and third parties are included.

3.5 The obligations on the Council, service areas, individual members of staff and councillors are explained.

3.6 The process for governance and review of the policy is clarified.

3.7 A list of supporting material which can be used in conjunction with this policy is provided.

4 SCOPE

4.1 In order to operate efficiently, Suffolk County Council (the Council) has to 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, the Council may be required by law to collect and use information in order to comply with the requirements of central government.

4.2 Personal information must be handled and dealt with properly, no matter how it is collected, recorded and used, and whether it is on paper, in computer records or recorded by any other means.

4.3 The Council regards the lawful and correct treatment of personal information as critical to its successful operations, maintaining confidence between the Council and those with whom it carries out business. The Council will ensure that it treats personal information correctly in accordance with the law.

4.4 The Council fully endorses and adheres to the principles of data protection as set out in the Data Protection Act 1998 (DPA).

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

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

4.7 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**.

4.8 This policy does not apply to information held by schools. If a request concerns the DPA in a school or a wish to access school records, the requester should contact the Head Teacher of the relevant school.

4.9 Elected Members should note that they are also data controllers in their own right, and are responsible for ensuring any personal information they hold/use in their office as Members is treated in accordance with the DPA.

4.10 The DPA 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.

5 THE PRINCIPLES OF DATA PROTECTION

5.1 The DPA stipulates that anyone processing personal data must comply with **eight principles** of good practice. These principles are legally enforceable.

5.2 The principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Act;
7. Shall be kept secure i.e. protected by an appropriate degree of security;
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

5.3 The DPA provides conditions for the processing of any personal data. It also makes a distinction between **personal data** and **"sensitive" personal data** (see glossary for definitions). Sensitive personal data requires stricter conditions of processing.

6 RESPONSIBILITIES

6.1 Suffolk County Council is a data controller under the Data Protection Act 1998. The Assistant Chief Executive is accountable for ensuring compliance with this policy.

The day-to-day responsibilities are delegated to the Head of Information Management.

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

6.3 Directors are responsible for ensuring that business areas they have responsibility for have processes and procedures in place that comply with the DPA and 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.

6.4 The Data Protection team, within Information Management, are responsible for providing day to day advice and guidance to support the Council in complying with the DPA and this policy.

6.5 Each SIA shall promote good practice and assist their Directorates in ensuring compliance with the DPA and this policy. The nomination of such a person shall not release other members of staff from compliance with the DPA and this policy.

6.6 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 the DPA.

6.7 The Council 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 Corporate Parenting
- Public Health - Assistant Director of Public Health

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

7 AGENTS, PARTNER ORGANISATIONS AND CONTRACTORS

7.1 If a contractor, partner organisation or agent of the Council 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 the Council, the lead Council officer

must ensure that personal data is kept in accordance with the principles of the DPA and this policy.

7.2 Security and Data Protection requirements must be included in any contract that the agent, contractor or partner organisation enters into with the Council.

7.3 A data exchange agreement must be in place prior to any work commencing. The Council promotes information sharing where it is in the best interests of the data subject.

7.4 The Council has information sharing protocols in place and will comply with the standards established in those protocols. Where appropriate, the Council's Caldicott Guardians will provide advice.

7.5 When information is shared with other organisations or partners, a formal information sharing agreement must be in place that is signed by all parties. Responsibility for its implementation lies with the Information Asset Owner. Guidance on Data Sharing Agreements can be found on the Information Management page available through Suffolk County Council's intranet.

7.6 Further advice and guidance is available by contacting the Information Management team.

8 ACCESS RIGHTS BY INDIVIDUALS - SUBJECT ACCESS REQUESTS (SARS)

8.1 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 under the DPA.

8.2 The Council provides information on how to make a SAR on the Council's website.

8.3 The statutory £10 fee is payable for all access to records applications.

8.4 All individuals who are or have been in the care of the council are exempt from the £10 fee.

9 DISCLOSURE OF PERSONAL INFORMATION ABOUT THIRD PARTIES

9.1 Personal data must not be disclosed about a third party, except in accordance with the DPA.

9.2 If you believe it is necessary to disclose information about a third party to a person requesting data, you must seek advice from the Information Management team.

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

10 INFORMATION SHARING

10.1 The Council 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.

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

10.3 The Council 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.

11 DATA QUALITY, INTEGRITY AND RETENTION

11.1 If an individual requests that personal data held about them be updated because it is wrong, incomplete or inaccurate, the position should be investigated thoroughly, with reference to the source of information.

11.2 A caution should be marked on the person's file to indicate uncertainty regarding accuracy until the investigation is complete.

11.3 The Council will work with the person to either correct the data and/or allay their concerns.

11.4 An individual is entitled to apply to the court for a correcting order which would authorise the Council to rectify, block, erase or destroy the inaccurate information as appropriate.

11.5 Individuals can request the Council to stop processing data. If data is properly held for marketing purposes for example, an individual is entitled to require that this is discontinued as soon as possible.

11.6 Requests must be made in writing, but generally all written or oral requests should be heeded as soon as they are made. The individual must be informed in writing that the processing has been discontinued ("cessation").

11.7 If data is held for any other purposes, an individual may request that processing ceases if it is causing them unwarranted harm or distress. This does not apply if they have given their consent, if the data is held in connection with a contract with the

person, if the Council is fulfilling a legal requirement, or, if the person's vital interests are being protected.

11.8 Valid written requests must be responded to in writing within 21 calendar days upon receipt.

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 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 in the DPA. However, this code does apply to the passing on of CCTV images to the media.

13 COMPLAINTS

13.1 Complaints about how the Council processes data under the DPA and responses to subject access requests are dealt with by an internal review.

13.2 Complaints are to be put in writing and sent to the Information Management team.

13.3 Contact details can be found on the SCC website under Privacy and Data Protection.

14 NOTIFICATION

14.1 The DPA requires every data controller processing personal data to notify and renew their notification on an annual basis. Failure to do so is a criminal offence.

14.2 The Information Commissioner maintains a public register of data controllers, in which the Council is registered.

14.3 The Information Management team will review and update the Data Protection Register annually prior to notification to the Information Commissioner.

14.4 Staff and elected Members should notify the Information Management team of any change to the processing of personal data between annual reviews.

15 BREACH OF POLICY

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

15.2 The Council will always treat any data breach as a serious issue, potentially warranting a disciplinary investigation.

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

16 REVIEW OF THE POLICY

16.1 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:

Information Management
Suffolk County Council
Constantine House
Constantine Road
Ipswich
Suffolk
IP1 2DH

17 FURTHER ADVICE

For further advice on this policy, please contact:

Your Strategic Information Agent, or

CIO Information Management Information.Management@suffolk.gov.uk