SUFFOLK COASTAL AND WAVENEY DISTRICT COUNCILS

DATA PROTECTION POLICY

CONTENTS

1. INTRODUCTION

1.1 Statement of Policy

1.1.1 This is a statement on the application of the Data Protection Act 1998 in the form of a policy, as adopted by the Corporate Management Team of Suffolk Coastal District Council (SCDC) and Waveney District Council (WDC) in August 2015.

1.2 Purpose of the Policy

1.2.1 The purpose of this document is to clearly acknowledge the Councils' responsibilities in relation to the Data Protection Act 1998.

1.2.2 This policy outlines the principles of the Data Protection Act 1998 and identifies how the Councils will comply with that Act.

1.2.3 Designated personnel and their responsibilities are identified.

1.2.4 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.

1.2.5 Procedure on accessing and disclosing personal information to individuals and third parties are included.

1.2.6 The obligations on the Councils, service areas, individual members of staff, elected Members, and agents are explained.

1.3 Scope of the Policy

1.3.1 In order to operate efficiently, SCDC and WDC have 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, customer, contractors, suppliers, and partner organisation. In addition, the Councils may be required by law to collect and use information in order to comply with the requirements of central government.

1.3.2 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.

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

1.3.4 The Councils fully endorse and adhere to the principles of data protection as set out in the Data Protection Act 1998.

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

1.3.6 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.

1.3.7 Elected Members should note that they are also data controllers in their own right, and are responsible for ensuring any personal information they hold or use in their office as elected Members is treated in accordance with the Data Protection Act.

1.3.8 The Data Protection Act 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 2000, but should also be considered fairly and lawfully.

2. THE PRINCIPLES OF DATA PROTECTION

2.1 The Data Protection Act stipulates that anyone processing personal data must comply with eight principles of good practice. These principles are legally enforceable.

2.2 The principles require that personal information:

- Shall be processed fairly and lawfully, and in particular, shall not be processed unless specific conditions are met;
- 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;
- Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed
- Shall be kept accurate and, where necessary, kept up to date;
- Shall not be kept for longer than is necessary for that purpose or those purposes;
- Shall be processed in accordance with the rights of the data subjects under the Act;
- Shall be kept secure i.e. protected by an appropriate degree of security; and
- Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures and adequate level of data protection.

2.3 The Data Protection Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and sensitive personal data. Sensitive personal data require stricter conditions of processing. Sensitive personal data includes, e.g. race, ethnic origin, political opinion, religious beliefs, trade union memberships, physical or mental health, sexual life, and offences, committed or alleged.

3. RESPONSIBILITIES

3.1 Suffolk Coastal and Waveney District Councils are data controllers under the Data Protection Act.

3.2 Through appropriate management and strict application of criteria and controls, SCDC and WDC will:

- Fully observe the conditions regarding the fair collection and use of personal data;
- Meet its legal obligations to specify the purposes for which personal data is used;
- Collect and process appropriate personal data, only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of personal data used;
- Apply strict checks to determine the length of time personal data is held;
- Take appropriate technical and organisational security measures to safeguard personal data;
- Ensure that personal data is not transferred abroad without suitable safeguards; and

- Ensure that the rights of people about whom personal data is held can be fully exercised under the Act. These include:
    - The right to be informed that processing is being undertaken;
    - The right of access to one's personal data;
    - The right to prevent processing in certain circumstances; and
    - The right to correct, rectify, block or erase personal data which is regarded as wrong information.

3.3 When handling personal information, SCDC and WDC will ensure:

- All employees and Councillors managing and handling personal data understand that they are responsible for following good data protection practice;
- Everyone managing and handling personal data is appropriately trained to do so;
- Everyone managing and handling personal data is appropriately supervised;
- Anybody wanting to make enquiries about handing personal data knows what to do;
- Methods of handling personal data are clearly described;
- A regular review and audit is made of the way personal data is managed;
- Methods of handing personal data are regularly assessed and evaluated;
- That the statutory 40 calendar day time limit is regarded as the maximum legal time to provide the information properly requested, and that SCDC and WDC employees must endeavour to provide that information without unnecessary delay;
- There is someone with specific responsibility for data protection in the organisation.

4. STAFF AND ELECTED MEMBERS

4.1 All members of staff and elected Members who hold or collect personal data are responsible for their own compliance with the Data Protection Act and must ensure that personal and / or sensitive information is kept and processed in accordance with the Data Protection Act and this policy.

4.2 All staff and elected Members must attend appropriate training courses and complete Data Protection training modules.

4.3 Staff and elected Members must not attempt to access personal data that they are not authorised to view. Failure to comply with the Data Protection Act may result in disciplinary action which could further lead to dismissal and, in some cases, criminal proceedings / prosecution.

4.4 Staff and elected Members must not use information obtained for personal gain or benefit, or pass this information onto others who might use it in such a way. Unauthorised disclosure of information of this kind may result in disciplinary action.

5. AGENTS, PARTNER ORGANISATIONS AND CONTRACTORS

5.1 If a contractor, partner organisation or agent of the Councils is appointed or engaged to collect, hold, process or deal with personal data on behalf of the Councils, or if they will do so as part of the services they provide to the Councils, they must ensure that personal data is kept in accordance with the principles of the Data Protection Act and this policy.

5.2 Security and Data Protection requirements must be included in any contract that the agent, contractor or partner organisation enters into with the Council. It is essential parties' security standards are equivalent to the Councils'.

5.3 A data exchange agreement must be in place prior to any work commencing. The Councils promote information sharing where it is in the best interests of the data subject and in compliance with the Data Protection Act.

6. ACCESS RIGHTS BY INDIVIDUALS – SUBJECT ACCESS REQUESTS (SARS)

6.1 An individual may request a copy of any data held about them, and information about the reasons for which it is kept and processed. This is called a Subject Access Request under the Data Protection Act.

6.2 The Councils provide information on how to make a Subject Access Request on their websites.

6.3 The statutory £10 fee is payable for Subject Access Requests.

6.4 Valid written requests will be acknowledged within 10 working days and a full response aims to be provided within 40 calendar days.

7. DISCLOSURE OF PERSONAL INFORMATION ABOUT THIRD PARTIES

7.1 Personal data must not be disclosed about a third party, except in accordance with the Data Protection Act.

7.2 If you believe it is necessary to disclose information about a third party to a person requesting data, you must seek advice from the Data Protection Officer.

7.3 All contractors and individuals working for or on behalf of the Councils must ensure identity checks are undertaken before providing personal data over the telephone in the course of normal service delivery.

8. INFORMATION SHARING

8.1 The Councils 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 The Councils 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 (see section 5.3).

9. DATA QUALITY, INTEGRITY AND RETENTION

9.1 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.

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

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

9.4 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.

9.5 Individuals can request the Councils to stop processing data in certain circumstances, but not for Council statutory duties, i.e. administration of Council Tax or electoral roll.

9.6 Personal data will be retained in accordance with the service area's retention policy.

10. CCTV MONITORING

10.1 Overt CCTV monitoring must be carried out in accordance with the Information Commissioner's Office's (ICO) code of practice on CCTV.

10.2 Any covert surveillance activities of the law enforcement community are governed by the Regulation of Investigatory Powers Act (RIPA) 2000, see the Head of Internal Audit for advice.

11. COMPLAINTS

11.1 All complaints concerning personal data must be put in writing and follow the Councils' complaint procedure.

11.2 If not satisfied after following the Councils' complaints procedure, the customer has the right of complaint to the ICO (www.ico.org.uk).

12. NOTIFICATION TO THE INFORMATION COMMISSIONER'S OFFICE

12.1 The Data Protection Act 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.

12.2 The Information Commissioner maintains a public register of data controllers, in which the Councils are registered, along with each elected Member.

12.3 The Data Protection Officer will review and update the Data Protection Register annually prior to notification to the Information Commissioner.

12.4 Staff and elected Members should notify the Data Protection Officer of any changes to the processing of personal data between annual reviews.

13. BREACH OF POLICY

13.1 The Councils will always treat any data breach as a serious issue, potentially warranting a disciplinary investigation or criminal proceedings. All perceived data breaches are to be reported to the Data Protection Officer.

14. FURTHER ADVICE

14.1 For further advice on this policy, please contact the Councils' Data Protection Officer, **Siobhan Martin**, Head of Internal Audit on 01394 444254 or email dataprotection@eastsuffolk.gov.uk.