Essex County Council Standards on Data Protection

Contents (view as PDF)

Title	Essex County Council Standards on Data Protection
Author/Owner	Information Management IS
Status	Final
Version	1.0
Date	March 2013
Review Date	March 2014
Security Classification	Not protectively marked
Approved by	Operations Board

1. Why do we need Standards for Data Protection?
1.1 The Council manages a great deal of information to undertake its day to day duties including information about people. The people this information relates to expect us to manage it safely and securely as if it was information about ourselves. Anyone using or processing the Council's information should ensure that they adhere to the eight data protection principles listed below from point 5 onwards.

1.2 Failure to comply with these Standards could result in:
- Physical harm to vulnerable people by leaking sensitive information; and
- A breach of the Data Protection Act which could result in penalties from the ICO including a fine of up to £500,000.

2. Responsibilities – All staff and anyone undertaking work on behalf of the Council, including Members
2.1 You have a responsibility to ensure that you act in accordance with the Data Protection Act 1998 (DPA) whenever you process information to do with living people, whether it is in relation to a citizen who uses our services or our employees. "Processing" means anything you do with information including, but not limited to, collecting, storing, sharing and destroying it.

2.2 If you receive a request for personal information, you must ensure that you process such in accordance with the guidance for handling requests for personal information. Also see point 8, principal 6 of these standards.

2.3 There are eight data protection principles which you must comply with by law. A brief summary of these principles is listed below, with some examples of what you must do to comply.

3. First principle: personal information is fairly and lawfully processed
3.1 You must only process personal information with the consent of the person or if the processing is necessary or if the processing satisfies another schedule 2 or schedule 3 condition. For example, it may be necessary to protect the life of an individual; to take action to meet our statutory or legal obligations, such as the protection of children or

vulnerable adults, or to prevent or detect crime. Other reasons are listed in the Act.

3.2 If you are collecting personal information, for example, to provide services or for a survey or a prize draw, you must tell people what you are going to do with it. You should do this by including a privacy notice (sometimes called a data protection statement) on the form used to collect the information.

3.3 As a minimum this should include, details of who is collecting the information (unless this is obvious), the purpose for collecting personal details, and whether you will be sharing it with anyone else. For full guidance on how to produce a privacy notice, please see Our Guide on How to Complete a Privacy Notice.

3.4 If the data is sensitive and consent is required, that consent must be "explicit", this means specific agreement to carry out a particular action. Sensitive personal data is defined in the Act and includes the following:

- Racial or ethnic origin
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of an offence
- Criminal proceedings

4. Second principle: personal information is processed for limited purposes

4.1 If information is collected for a specific purpose, our use of that information must be limited to that purpose or one very closely linked to it. For example, to register members of the public for a blue badge, that information must not be used as a mailing list for adult learning, however it could be used to inform people of changes to the blue badge service. Organisations that process personal information are required to notify the Information Commissioner's Office (ICO) of the purposes for which they use it, which are published in the ICO's register. Information Management IS (IMIS) does this for ECC.

5. Third principle: personal information is adequate, relevant and not excessive

5.1 You must only collect and/or hold the minimum amount of information you need to carry out our business purpose. It is not acceptable to hold information on the basis that it might possibly be useful in the future without a view of how it will be used. Changes in circumstances or failure to keep the information up to date may mean that information that was originally adequate becomes inadequate. If information is kept for longer than necessary then it may be both irrelevant and excessive.

6. Fourth principle: personal information is accurate and kept up to date

6.1 You must take reasonable steps to ensure the data you hold is accurate, up to date and not misleading. For example, whenever contact is re-established with a citizen, you should check that the information you hold about them is still correct.

7. Fifth principle: personal information is not kept for longer than is necessary

7.1 You should review personal data regularly and delete information which is no longer required, although you must take account of statutory and recommended minimum retention periods. Subject to certain conditions, the Act allows us to keep indefinitely personal data processed only for historical, statistical or research purposes. ECC has a retention schedule that gives guidance in this area.

8. Sixth principle: personal information is processed in line with an individual's rights

8.1 People have a number of rights under the DPA which are listed in full in the Act itself and on the ICO website. These rights include, but are not limited to:

- the right to access to your own personal information;
- the right to prevent processing likely to cause damage or distress;
- the right to have information corrected or deleted; and
- the right to complain to the Information Commissioner.

8.2 Everyone's rights under the Act must be respected, although there are limited circumstances defined in the Act when our other responsibilities as a public authority override a person's rights, for example, if you are required to share information for the protection of children.

8.3 Anyone, including employees, can ask for the information ECC holds about them, which is known as a subject access request (SAR), and we have a maximum of 40 calendar days to provide the requested information. A subject access request form is available on request but use of this is not mandatory, although the request must be made in

writing and evidence of identity must be provided.

8.4 Our guide, 'How to recognise a request for information' helps you understand whether a request for information is a SAR and there is guidance on handling SARs which gives further details and explains what you must do if you are involved in responding to one. If you receive a SAR, you must pass it immediately to the Access to Records Team, who handle SARs for the whole of ECC. We do not charge for subject access requests.

9. Seventh principle: personal information is kept secure

9.1 You must take steps to ensure that personal information is protected, so that only those people who need it for their job can access it. This includes:

- technical methods, such as encryption, password protection of systems, restricting access to network folders;
- physical measures, such as locking cabinets, keeping equipment like laptops out of sight, ensuring buildings are physically secure; and
- organisational measures, such as providing proper induction and training so that staff know what is expected of them and taking reasonable steps to ensure the reliability of staff that access personal data, for example, by the use of CRB checks.

9.2 The Essex Service Desk knowledgebase contains a number of "How to" guides which will help in these areas. The following standards give further information on how to keep information secure:

- Our standards for portable equipment and information management
- Our standards for physical security including buildings, information and equipment storage, CCTV and re-organisation of services
- Our standards for acceptable use and behaviours when using information technology.

10. Eighth principle: personal information will not be transferred to other countries without adequate protection

10.1 Data is protected in most European countries. Many other countries are not considered to have adequate protection for personal data. If sending information to another country, check the ICO's website or contact IMIS to confirm that sending the information complies with this principle.

11. Protecting the personal data of ECC employees

11.1 As noted under the sixth principle above, ECC employees are able to request the information ECC holds about them by submitting a subject access request.

11.2 Please note that some information ECC holds about employees is considered business information, not personal information, which means it could be released if requested under the Freedom of Information Act 2000. This includes information such as: job title; salary band; work telephone number; work address. If you have concerns over this type of business information being disclosed please contact your manager or Information Management IS.

12. Further Information

12.1 For further information or training on the DPA, contact the Information Management team (IMIS) on 01245 431851 or by email on information.management@essex.gov.uk

12.2 The ICO publishes detailed information about our legal obligations under the DPA and the full text of the Act can be viewed on the www.legislation.gov.uk site

12.3 The Department for Education (DfE) has some useful information about sharing information.

12.4 The Essex Trust Charter holds details of our current Information Sharing Protocols with partner agencies, along with guidance.

13. Applicable Controls and References for Audit Purposes

- PSN IA Conditions – Annex A Example Acceptable Use Statements
- SPF-MR1, MR2 – HMG Security Policy Framework v8 Mandatory Requirement
- HAN-1.1, HAN-1.2 – Hannigan: Mandatory Minimum Measures
- IS0-6.1.1, 6.1.2 - ISO27001
- IAS6-2, IKAS6-4 – HMG IA Standard No6
- NHS-101, 104 – NHS Information Governance Toolkit
- PSN-ACC1, ACC2 – PSN Code of Connection v2.0
- PCI-8, PCI-12 – Payment Card Industry Data Security Standard v2.0
- Essex County Council Information Management Policy
- Essex County Council Information Security Policy Statement

• Essex County Council Standards for physical security including buildings, information and equipment storage, CCTV and re-organisation of services
• Essex County Council Standards for acceptable use and behaviours when using information technology
• Essex County Council Standards for Payment Card Security

(ISO-15.1.4, MR6, MR7, MR8, NHS102)

14. Approval and updating
These Standards are developed in conjunction with IPDG and approved by the Operations Board. They will be reviewed annually, and any proposed amendments will be submitted to the appropriate governance point for consideration and approval