Data Protection Policy

Version 4.0
Policy Date: 06/04/10
Information Governance Team
Strategic Intelligence
Office of the Chief Executives

If you require help in the interpretation of this policy, contact the Corporate Information Governance Manager at keepdevonsdatasafe@devon.gov.uk

If this document has been printed please note that it may not be the most up-to-date version. For current guidance please refer to The Source.

This policy can be made available to the public, upon request, under the Freedom of Information Act 2000.

Contents

Introduction

The Data Protection Act 1998 (DPA 1998) establishes a framework of rights and duties which safeguard personal data. Personal data is information about a living individual, who can be identified from the data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes, against the right of individuals to respect, for the privacy of their personal details.

Devon County Council is committed to protecting the privacy of individuals and handles all personal data in a manner that complies with the DPA 1998. The Council has established the following policy to support this commitment. It is the **personal responsibility** of all employees (temporary or permanent), Members, contractors, agents and anyone else processing information on our behalf to comply with this policy.

Any deliberate breach of this policy could amount to a criminal offence under one or more pieces of legislation, for example the Computer Misuse Act 1990 and the DPA 1998. All incidents will be investigated and action may be taken under the Council's formal disciplinary procedure. A serious breach of this policy could be regarded as gross misconduct and may lead to dismissal and / or criminal action being taken.

This policy explains what our expectations are when processing personal data. This policy should be read alongside the Personal Information Security Policy and the Corporate Disposal Policy which is available on the Keep Devon's Data Safe web page on the Source.

1.0 Data protection principles

1.1 The DPA 1998 is underpinned by a set of eight common-sense principles, which must be adhered to whenever personal data is processed. Processing includes obtaining, recording, using, holding, disclosing and deleting personal data.

A summary of the data protection principals is as follows:

Personal data must be:

- processed fairly and lawfully
- processed for specified and lawful purposes
- adequate, relevant and not excessive

- accurate, and where necessary kept up to date
- not kept longer than is necessary
- processed in accordance with the rights of the data subject
- kept secure
- transferred only to countries with adequate security

Information about what the principles mean can be found on the Data Protection pages on the Source.

2.0 Access and use of personal data

2.1 Access and use of personal data held by the Council, is only permitted by employees (temporary or permanent), Members, contractors, agents and anyone else processing information on our behalf, for the purpose of carrying out their official duties. Use for any other purpose is prohibited. Deliberate unauthorised access to, copying, destruction or alteration of or interference with any computer equipment or data is strictly forbidden.

3.0 Collecting personal data

3.1 When personal data is collected, for example on a questionnaire, survey or a form, the data subject (that is to say the person who the information is about) must be told, unless this is obvious to them, which organisation(s) they are giving their information to; what their information will be used for; who it may be shared with and anything else that might be relevant e.g. the consequences of that use. This is known as a Privacy Notice.

3.2 A template Privacy Notice can be found on the Data Protection web pages on the Source. Further guidance and assistance in creating a Privacy Notice, can be obtained from the Information Governance Team, in Strategic Intelligence on 01392 38(4678).

3.3 Personal data collected, must be adequate, relevant and not excessive for the purpose of the collection. A person's name and other identifying information should not be collected where depersonalised (anonymous) information would suffice.

3.4 If the information is collected for one purpose, it cannot subsequently be used for a different and unconnected purpose, without the data subject's consent (unless there is another lawful basis for using the information (see section 4 below)). It must be made clear to the data subject

at the time the information is collected, what other purposes their information may be used for.

4.0 Lawful basis for processing

4.1 When Devon County Council processes personal data, it must have a lawful basis for doing so. The DPA 1998 provides a list of 'conditions' when we can process personal or 'sensitive' personal data and are contained within Schedule 2 and Schedule 3 of the Act. A summary of these conditions can be found on the Data Protection pages on the Source.

4.2 The DPA 1998 defines sensitive personal data as information relating to a person's racial or ethnic origin; political opinion; religious or other beliefs; trade union membership; physical or mental health or condition; sexual life; criminal offences (alleged or committed).

4.3 Whenever the Council processes personal data, it must be able to satisfy at least one of the conditions in Schedule 2 of the DPA 1998 and when it processes 'sensitive' personal data, it must be able to satisfy at least one of the conditions in Schedule 3 of the DPA 1998 as well.

4.4 As an example, Devon County Council can process personal data if it:

- is necessary to comply with a legal obligation
- is necessary to protect someone's life or to protect them from serious harm
- is in the public interest and is necessary for the Council or another organisation to undertake its official duties
- is necessary for a legitimate and lawful purpose and does not cause unwarranted prejudice to the data subject
- is necessary to assist in the prevention or detection of an unlawful act

4.5 The Council can also process personal data if it has the data subject's consent (this needs to be 'explicit' when it processes sensitive personal data). In order for consent to be valid it must be 'fully informed' which means the person giving consent must understand what they are consenting to and what the consequences are if they give or refuse consent. Consent must not be obtained through coercion or under duress. More information about consent can be found on the Knowing When To Share pages on the Source.

5.0 Disclosing personal data

5.1 Personal data must not be disclosed to anyone internally or externally, unless the person disclosing the information is fully satisfied that the enquirer or recipient is authorised in all respects and is legally entitled to the information.

5.2 If personal data is disclosed to another organisation or person outside of the Council, the disclosing person must identify their lawful basis for the disclosure (see section 4 above) and record their decision. This should include a description of the information disclosed; the name of the person and organisation the information was disclosed to, the date, the reason for the disclosure and the lawful basis.

5.3. If an information sharing agreement or protocol exists, this should be adhered to. More information about sharing information with other organisations can be found on the Knowing When To Share pages on the Source. Guidance on disclosing information to the Police and other law enforcement agencies is also available on these pages.

5.3 In response to any lawful request, only the minimum amount of personal information should be disclosed. The person disclosing the information should ensure that the information is adequate for the purpose of the disclosure, relevant and not excessive.

5.4 When personal data is disclosed internally or externally, it must be disclosed in a secure manner. More information about how to disclose information securely by phone, fax, letter or email, can be found on the Keep Devon's Data Safe pages on the Source.

6.0 Accuracy and relevance

6.1 It is the responsibility of those who receive personal information to ensure so far as possible, that it is accurate and up to date. Personal information should be checked at regular intervals, to ensure that it is still accurate. If the information is found to be inaccurate, steps must be taken to rectify it. Individuals who input or update information must also ensure that it is adequate, relevant, unambiguous and professionally worded. Data subjects have a right to access personal data held about them and have inaccuracies corrected. More information about a data subject's rights can be found in Section 8 below.

7.0 Retention and disposal of data

7.1 Devon County Council holds a vast amount of information. The DPA 1998 requires that we do not keep personal data for any longer than is necessary. Personal data should be checked at regular intervals and deleted or destroyed when it is no longer needed, provided there is no legal or other reason for holding it.

7.2 The Corporate Record Retention Policy must be checked before records are disposed of, to see whether there is a prescribed retention period for that type of record. Specific advice on record retention should be obtained from the Corporate Information Manager. More information about Records Management can be found on the Source.

7.3 When disposing of information, equipment or media, the Corporate Disposal Policy should be adhered to. This policy is available on the Keep Devon's Data Safe pages on the Source.

8.0 Individual's rights

8.1 Individuals have several rights under the DPA 1998. These include the right to access personal data held about them (this is known as Subject Access); the right to prevent their information being used in a way which is likely to cause damage or distress; the right to compensation for any damages as a result of their information not being handled in accordance with the DPA 1998; and the right to have inaccurate or misleading information held about them, corrected or destroyed. A person wishing to exercise any of these rights must be given the Information Governance Team's contact details, which can be found on the data protection page on the public website.

8.2 It is particularly important that if a person has made a Subject Access request that this is forwarded to the Information Governance Team as soon as possible. The council has 40 calendar days in which to respond to a Subject Access request, provided the applicant has put their request in writing and suitable identification has been supplied. More information about Subject Access requests can be found on the data protection pages on the Source.

9.0 Reporting security incidents

9.1 Devon County Council has a responsibility to monitor all incidents that occur within the organisation that may breach the security and/or the confidentiality of its information. All incidents need to be identified, reported, investigated and monitored. It is only by adopting this approach that the Council can learn from its mistakes and prevent losses re-occurring.

9.2 The Council has developed and implemented an Information Security Incident Reporting Policy. If information has been lost, found or stolen (including the loss or theft of laptops, Blackberries, Smartphones etc) this must be reported to the Information Governance Team and the Security Incident Reporting Form completed.

This Policy is owned by the Corporate Information Governance Manager and will be reviewed on an annual basis.

For help in interpreting this policy, contact the Corporate Information Governance Team on 01392 384682 or email keepdevonsdatasafe@devon.gov.uk.

Policy History

Policy Date	Summary of Change	Contact	Implementation Date
18/03/10	This policy has been completely re-written to take into account new policies, guidance and processes which support the Data Protection Policy. A copy of the V3 2007 DP Policy can be obtained from the Information Governance Manager.	A Steer-Frost, Information Governance Manager, County Hall, Exeter.	18/03/10