Data Protection Policy

Version 7.0
Policy Date: 20/12/13
Customer Relations and Information Governance Service
Business Strategy and Support

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 must not be disclosed outside of Devon County Council without permission from the Information Governance Manager – email dpoffice@devon.gov.uk

Reviewed by Resources Committee 04.05.17

1. Introduction

1.1 This policy sets out Devon County Council's (the Council) commitment to handling personal data in accordance with the Data Protection Act 1998 (the Act). The Council is registered under the Act with the Information Commissioner's Office (ICO)-registration number Z6475582. Full details of the Council's registration can be found at www.ico.gov.uk.

2. Purpose

2.1 This policy sets out the Council's approach to handling personal data and developing a security-conscious culture throughout the organisation. It informs all persons who process personal data on the council's behalf of their obligations when handling its data. This policy is part of a suite of information governance related policies and guidance developed to protect the Council's information assets, which must be read alongside this Data Protection Policy. An index of these policies and guidance are in section 7 of this policy.

3. Scope

3.1 This policy applies to all Council employees, agency staff, contractors, Members and third party staff, who process personal data on behalf of the Council.

3.2 Where this policy reads "staff", it should be read to include all the entities in paragraph 3.1 above.

3.3 This policy continues to apply to staff even after their relationship with the Council ends.

4. Roles and responsibilities

4.1 The Council's data protection obligations are managed and maintained by the Information Governance Manager, who acts as the County Data Protection Officer. Overall responsibility for organisational Data Protection compliance rests with the Council's Senior Information Risk Officer (SIRO).

4.2 All staff are personally responsible for complying with the act and this Data Protection Policy, and must ensure the information they have access to, handle and share, is processed lawfully, securely and professionally.

4.3 Any reckless or deliberate breach of this policy will result in disciplinary action and in very serious cases, could lead to criminal or civil action being taken against the staff member concerned.

4.4 Advice on the handling and sharing of personal data in compliance with the Data Protection Act, can be obtained from the Information Governance Team at dpoffice@devon.gov.uk or on 01392 38(3027). Written guidance can also be found on the *Keep Devon's Data Safe* web pages and the *Knowing When to Share* web pages on the Source.

5. Policy content

5.1 The Data Protection Principles

5.2 The Act is underpinned by a set of eight common-sense principles, which governs the way the Council processes personal data. Personal data means data which relates to a living individual who can be identified from that data or other information held by the Council. All staff who *process* e.g. collects, uses, stores, accesses, discloses etc. personal data, must do so in accordance with these principles.

5.3 Section 5 sets out how the council complies with each of these principles and its expectations of staff when handling personal data.

5.4 A summary of the data protection principles is as follows:

Personal data shall 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 data subjects*
- *kept secure*
- *transferred only to countries with adequate security*

5.5 Fair and lawful

5.6 The first principle requires the council to be *fair* by being open and transparent with individuals (i.e. data subjects) about how their personal data is going to be collected, used, held, shared etc. and any non-obvious consequences of that use. This is known as *fair*

processing or providing a *Privacy Notice*.

5.7 In order to meet this requirement, when the council collects or shares personal data, it will tell those individuals what will happen to their information, by way of a *Privacy Notice*. This may be provided in writing, for example in a public leaflet; a notice on the council's website; on a form when the information is collected or in some cases verbally, for example on a recorded message on the Customer Service Centre Public Helpline or during a conversation between a staff member and the individual whose personal data is being processed.

5.8 All staff who collect personal data for example on a questionnaire, survey or form or who want to share personal data with a third party, must notify the individual (unless in doing so it would put someone at risk or prejudice a criminal investigation) and provide them with an appropriate Privacy Notice. A template Privacy Notice is available on the *Keep Devon's Data Safe* pages on the Source for staff to use and adapt. Further advice and guidance can be obtained from the Information Governance Team at dpoffice@devon.gov.uk

5.9 The first data protection principle also requires the council to have a legal basis for processing personal data and provides a list of *conditions* in Schedule 2 of the Act. The council must be able to satisfy at least one condition from this schedule for its processing of personal data to be lawful. In the case of *sensitive* personal data (i.e. information that relates to a person's racial or ethnic origin; political opinion; religious beliefs; trade union membership; physical or mental health or condition; sexual life and criminal offences (alleged or committed)) the council must also satisfy at least one condition in Schedule 3 of the Act as well.

5.10 A summary of some of the conditions which the council abides by when it processes personal and *sensitive* personal data is as follows:

The processing is:

- *in the public interest and is necessary for the Council or another organisation to undertake its official duties;*
- *legitimate and lawful and does not cause unwarranted prejudice to the data subject;*
- *with the data subject's consent;*
- *necessary to protect someone's life or to protect them from serious harm;*
- *necessary to comply with a legal obligation; and*

- *necessary to assist in the prevention or detection of an unlawful act and in the administration of justice.*

5.11 For guidance on sharing or requesting personal data from organisations, visit the *Knowing When to Share* web pages on the Source or telephone 01392 38(3027).

5.12 Requests for information from the Police or other organisations for crime prevention or detection purposes, must be sent to the Information Governance Team. For advice and instructions please contact 01392 38(3027). Guidance on disclosing information to the Police and other law enforcement agencies is available on the Knowing When To Share pages on the Source.

5.12 For advice on identifying the lawful basis for collecting, using and sharing personal or *sensitive* personal data, or queries in relation to this, contact the Information Governance Team at dpoffice@devon.gov.uk.

5.13 Specified and lawful purposes (limited purposes)

5.14 This principle requires the council to process personal data for the purpose or purposes in which it was intended. In simple terms, the council must not collect personal data for one purpose and then use it for something *completely different* and *unconnected*, unless it is reasonable and lawful to do so. Staff must ensure they use personal data in the way individuals would reasonably expect and in accordance with the Council's Privacy Notices and Data Protection Registration.

5.15 Adequate, relevant and not excessive

5.16 The council and its staff are required to ensure that any personal data it processes is *adequate* (fit for purpose), *relevant* and *not excessive* (is not more than is required for the particular purpose(s)). All staff are required to apply this common-sense principle to their every-day working practices when they collect, use and share personal data.

5.17 Accurate and up to date

5.18 Staff must take reasonable steps to ensure that any personal data they record is accurate and where required, kept up to date. Personal data that may be subject to change, for example home addresses, contact telephone numbers etc., 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. Where personal data is shared, staff must take reasonable steps to ensure it is accurate and current, prior to sharing the data or notify the recipient if it is not clear whether the

information is up to date. Complaints from data subjects regarding the accuracy of their personal data held by the council, should be handled by the relevant department and service area responsible for the information.

5.19 Not kept for longer than necessary

5.20 The council is not permitted to keep personal data for any longer than it needs to and must ensure that information is deleted or destroyed when it is no longer required, provided there is no legal or other reason for requiring its retention. To assist in this process the council has a Record Retention Policy and a Corporate Disposal Policy which stipulates how long the Council will hold certain records for and how it will dispose of them. Staff must ensure they follow these policies and destroy personal data when it is no longer required, in a secure and appropriate manner. For advice on how long to keep records for, contact the Information Manager on 01392 38(4673).

5.21 Rights of data subjects

5.22 The Act provides several rights to data subjects (i.e. individuals who the council holds personal data about). In summary, these rights include (but are not limited to) the following:

- *the right to request a copy of any personal data held about them* (these are known as 'Subject Access Requests');
- *the right to prevent processing likely to cause damage or distress* (these are known as 'Section 10 Notices');
- *the right to prevent processing for direct marketing purposes*;
- *the right to compensation for damage caused as a result of the data controller failing to comply with certain requirements of the Data Protection Act* (e.g. resulting from personal data security breaches); and
- *the right to have inaccurate or misleading information corrected, deleted or the records updated to show the data subject's views*

5.23 The Information Governance Team is responsible for managing all Subject Access requests and Section 10 Notices. Requests and Notices should be made in writing and sent to the Information Governance Team at County Hall, Room 120, Topsham Road, Exeter, EX2 4QD or dpoffice@devon.gov.uk

5.24 Complaints, comments and feedback from data subject's regarding their personal data, should be made in writing and sent to the Customer Relations Team at Room 120, County Hall, Topsham Road, Exeter EX2 4QD or customer.relations@devon.gov.uk

5.25 The Council's procedure for handling Subject Access Requests and Section 10 Notices are available on the *Keep Devon's Data Safe* pages on the Source.

5.26 Advice on data subject's rights under the Act can be obtained from the Information Governance Team on 01392 38(3027).

5.27 Keeping personal data secure

5.28 The council takes its data protection security obligations under the Act very seriously and has in place appropriate technical and organisational measures to protect the personal data it holds and is responsible for, from unauthorised or unlawful processing and against accidental loss, destruction or damage.

5.29 The council ensures the reliability of its employees who have access to personal data, by ensuring that all employment checks are made and references are obtained for *desired candidates,* prior to any appointments being made. Some roles within the council will also require a Disclosure and Barring Service (DBS) check to be carried out on the individual. In such cases, this will be made clear to candidates on job advertisements.

5.30 Managers must ensure they follow the Induction Checklist for Managers on the Source, for all new employees, and ensure the individual is fully aware of their obligations for *Keeping Devon's Data Safe*. All employees, agency staff, contractors and other relevant staff must sign the Data Protection Policy Declaration (at Appendix 2) and agree to process personal data in accordance with this Policy, before being given access to any sensitive council data.

5.31 It is mandatory for all new employees, temporary agency staff and contractors who process personal data, to complete the Council's Data Protection e-training prior to being given access to sensitive information. It is also mandatory for all existing employees to undertake refresher Data Protection training every two years. Managing and monitoring this is the responsibility for all managers.

5.32 Staff who work in People Services are required to complete the Information Sharing E-training, in addition to the Data Protection E-training, within the first month of their induction.

5.33 The Data Protection and Information Sharing E-training is available via the *Keep Devon's Data Safe* pages on the Source. Printable versions of the training are also available on these pages, for individuals who have difficulty in undertaking the training on-line.

5.34 All staff are personally responsible for ensuring they take appropriate and reasonable steps to secure the personal data they have access to, and must follow the council's policies and guidance in relation to this.

5.35 Staff are given access to the Council's data on a strict need to know basis, for the purpose of carrying out their official duties for the council. Section 55 of the Act makes it an offence for a person to knowingly or recklessly, without the consent of the data controller (the Council), obtain or disclose personal data, or procure the disclosure of the data to another person. There are some exceptions to this, for example if the obtaining, disclosure or procuring can be justified in the public interest. There is also a similar offence under Section 1 of the Computer Misuse Act 1990. This does not affect individuals rights under the Public Interest Disclosure Act 1998 (Whistleblowing). The Council's Whistleblowing Policy is available on the Source.

5.36 All staff must ensure that their access to personal data and computer systems and any processing they carry out, is appropriate, authorised and lawful at all times. Failure to do so will result in disciplinary action, and in serious cases, criminal action being taken against them.

5.37 The council recognises that on occasion, unfortunate incidents may occur when personal data or sensitive/confidential business data or equipment may be put at risk. In the event of staff becoming aware of such instances, they must notify the Information Governance Team immediately, using the Incident Reporting Form available via the *Keep Devon's Data Safe* pages on the Source. All incidents will be identified, reported, investigated and monitored. It is only by adopting this approach that the Council can learn from its mistakes and prevent incidents re-occurring.

5.38 All incidents will be handled in accordance with the Council's Security Incident Management Policy and Procedure. In the event of a serious incident, staff must report the incident to the Information Governance Team by telephone, on 01392 38(0100) as well as reporting it via the Incident Reporting Form.

5.39 There are times when the council needs to disclose personal data to third parties so they can carry out a service or work on behalf of the council, under its instruction. These third parties are known as 'data processors'. Where a data processor is used, the Council must ensure it chooses a data processor who can provide sufficient security guarantees in respect of the personal data it will be processing on behalf of the council.

5.40 All staff who instruct a data processor, must ensure they carry out the necessary security checks before any personal data is disclosed. A template security questionnaire is available on the *Keep Devon's Data Safe* pages on the Source for staff to adapt accordingly, and data processors to complete. Advice should be obtained from the Information Governance Team at keepdevonsdatasafe@devon.gov.uk on when to use this security questionnaire and whether some of the questions are necessary and to have the answers evaluated.

5.41 Staff must also ensure that when instructing a data processor they issue them with a written contract (Data Processor Agreement) stipulating their obligations to keep the council's data secure. This must be signed by the data processor before they receive access to the council's data. Failure to do so will result in a breach of the Data Protection Act with potential serious consequences.

5.42 A template Data Processor Agreement (DPA) is available on the *Keep Devon's Data Safe* pages on the Source, for staff to adapt accordingly. Advice on when to use a DPA can be obtained from the Information Governance Team at dpoffice@devon.gov.uk

5.43 Transferring personal data over-seas

5.44 The Act requires that when transferring personal data to a country outside the European Economic Area (EEA) it is only permitted if that country or territory can ensure an adequate level of protection for the rights and freedoms of data subjects. This principle becomes particularly relevant in cases where staff want to, or need to email personal data to a country/territory outside the EEA, or if they want to collect, store or share the data on a web based platform, for example via an on-line questionnaire or on a file sharing website.

5.45 Staff who want to collect, share, store or email personal data outside the EEA, must discuss this beforehand with the Information Governance Team on 01392 38(0100) and follow the guidance on Transferring Personal Data Outside the EEA, on the *Keep Devon's Data Safe* pages on the Source.

6. Privacy Impact Assessments

6.1 There may be times when the council decides to transfer or take on additional services or undertake new initiatives, which involves the processing of large amounts of personal data (whether staff, service user or customer data) . In such cases the council will be required to assess the risks, legal implications and impact this will have on the council and data subjects.

6.2 The Information Governance Team must be consulted at the start of any new project or initiative where large amounts of personal data will be processed. This includes the transferring, merging, sharing, storage and transmission of personal data.

6.3 The Information Governance Team will carry out Privacy Impact Assessments or Privacy Law Compliance Checks as and when required. Contact this team on 01392 38(3027) or dpoffice@devon.gov.uk for advice and guidance in relation to this.

7. Policy History

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

8.2 For help in interpreting this policy, contact the Information Governance Team on 01392 38(3027) or email dpoffice@devon.gov.uk

Policy Date	Summary of Change	Contact	Implementation Date
01/12/2013	This policy has been re-written to take into account new policies, guidance and processes which support this Data Protection Policy. Previous policy versions are available upon request.	A Steer-Frost, Information Governance Manager, County Hall, Exeter.	20/12/2013
22/02/2011	Insertion of a new sentence in the 2nd paragraph in the Introduction: 'This policy continues to apply to employees and individuals, even after their relationship with the Council ends'	A Steer-Frost, Information Governance Manager, County Hall, Exeter.	22/02/2011
15/09/10	Insertion of paragraphs 2.2, 2.3 and 2.4. Removal of the following sentence from 4.1: 'A summary of these conditions can be found on the Data Protection pages on the Source'.	A Steer-Frost, Information Governance Manager, County Hall, Exeter.	15/09/10
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 Corporate Information Governance Manager.	A Steer-Frost, Information Governance Manager, County Hall, Exeter.	18/03/10

Appendix One

Policy and Guidance Index

7.1 This Data Protection Policy should be read alongside the following policies and guidance:

Policy Name	Document Owner	Document Location
Personal Information Security Policy	Senior Information Risk Officer	Keep Devon's Data Safe, The Source
Corporate Disposal Policy	Senior Information Risk Officer	Keep Devon's Data Safe, The Source
Security Incident Management Policy	Senior Information Risk Officer	Keep Devon's Data Safe, The Source
Freedom of Information and Environmental Information Request Handling Policy	Senior Information Risk Officer	Keep Devon's Data Safe, The Source
Publishing Information on the Web Policy	Senior Information Risk Officer	Keep Devon's Data Safe, The Source
Mobile Working Security Policy	Senior Information Risk Officer	ICT Policies and Guidelines, The Source
Email Policy	Senior Information Risk Officer	ICT Polices and Guidelines, The Source
Using and Participating In Social Media Policy	Head of Human Resources	HR Guidance and Policies, The Source
Corporate Homeworking Policy	Head of Human Resources	HR Guidance and Policies, The Source
Strategic Information and Records Management Policy	Head of Strategic Intelligence	Insight and Impact, The Source
Personal Information Management Policy	Head of Strategic Intelligence	Insight and Impact, The Source

Guidance Name	Document Owner	Document Location
Guide for Carrying Paper Files Off-Site	Senior Information Risk Officer	Keep Devon's Data Safe, The Source
Information in Future Delivery Models	Senior Information Risk Officer	Keep Devon's Data Safe, The Source
Sending Information by Post, Email, Fax or Phone	Senior Information Risk Officer	Keep Devon's Data Safe, The Source
Security Articles Published in Insider	Senior Information Risk Officer	Keep Devon's Data Safe, The Source
Using County Council Websites and Internet Guidance	Senior Information Risk Officer	ICT Polices and Guidelines, The Source
Use of Telephones and Faxes Guidance	Senior Information Risk Officer	ICT Policies and Guidelines, The Source
Using Your Computer Guidelines	Senior Information Risk Officer	ICT Policies and Guidelines, The Source
Private Use of ICT Guidelines	Senior Information Risk Officer	ICT Policies and Guidelines, The Source
Camera and Camera Phones Guidelines	Senior Information Risk Officer	ICT Policies and Guidelines, The Source
Email Guidelines	Senior Information Risk Officer	ICT Policies and Guidelines, The Source

Appendix Two

Data **Protection** Policy Declaration

To be completed by all employees, agency staff, contractors and other relevant staff who process personal data on behalf of Devon County Council.

Managers must keep a copy of the signed Declaration on the employee's central Personnel File or other relevant and accessible file for non employees.

Declaration

I confirm that I have read, understood and will adhere to Devon County Council's Data Protection Policy.

Signed: ……...

Printed: ……...

Line Manager's name: ……...

Department/section: ……

Service: ……

Date: ……...