COTSWOLD DISTRICT COUNCIL

COTSWOLD DISTRICT COUNCIL

DATA PROTECTION POLICY

Contents

Document Control

Version	Date	Author	Comments
1	June 2017	ICT Audit and Compliance Manager	ICO Compliance

Policy Statement

This Policy describes the Council's requirements to comply with Data Protection.

The Data Protection Act 1998 (DPA) was introduced to protect the interests of individuals. The legislation covers **both** electronic information and manual files the Council holds.

The Council processes and keeps personal information about its customers so that it can provide them with the services they require.

The Council must comply with the 8 Data Protection Principles:

The information must be:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the European Economic Area without adequate protection

Scope

This document applies to all Councillors, Committees, Services, Partners, employees of the Council, contractual third parties and agents of the Council who use ICT facilities and equipment remotely, or who require remote access to the Council's Information Systems or information.

This Policy applies to all information which is subject to the Data Protection Act 1998 including;

- all personal data this is processed automatically
- any personal data held in a manual form in a relevant filing system
- any personal data held in an accessible record

The Policy should be applied with appropriate reference to the Council's ICT policies including, but not restricted to, the following:

Access Control Policy
Card Payments Standards Policy
Email Usage Policy
GCSx Acceptable Usage Policy
Incident Management Policy
Information Protection and Handling Guidance
Information Security Standards Policy
Equipment Usage Policy
Internet Usage Policy
Removable Media Policy
Software Security Policy

Objective

The Policy aims to ensure that personal data is processed fairly and lawfully.

The Council must comply with all relevant legislation and good practice to protect the personal data held, and to monitor and review compliance with legislation and introduce changes where necessary.

Those who process data must respect the confidentiality of all personal data, and the Policy provides staff with appropriate procedures to handle such data.

This Policy also aims to outline the rights of members of the public in gaining access to their personal data held by the Council, and to assist the Information Commissioner Office (ICO) and the external auditor as required.

Risks

The Council recognises that there are risks associated with users processing and handling information in order to conduct official Council business.

This Policy aims to mitigate the followings risks:

- Accidental or deliberate breach of data protection.
- Potential sanctions against the Council or individuals imposed by the ICO as a result of the loss or misuse of data. The Council could be required to a pay a fine up to £500k for serious breaches.
- Potential legal action from data subjects based on a breach of data protection.
- Council reputational damage as a result of a data protection breach.

Definitions

Data Controller - The person(s) who determines how and the manner in which personal data are or are to be processed (the Council).

Data Processor - The person who processes the data on behalf of the data controller.

Data Subject - The person who the personal information is about.

Data Sharing - The ability to share the same data resource with multiple applications or users. It implies that the data are stored in one or more servers in the network and that there is some software locking mechanism that prevents the same set of data from being changed by two people at the same time

Data Protection Officer (DPO) - A Data Protection Officer (DPO) is a person in charge of ensuring an organisation's compliance with the Data Protection Act 1998.

Information Commissioner's Office (ICO) - The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Information Asset Owner – A senior member of staff who is the nominated owner for one or more assets, by virtue of managerial position.

Personal data - Information relating to living people who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

Processing data - Includes obtaining, sharing, disclosing, recording, holding, using, erasing or destroying personal information.

Personal Data Breach - A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service.

Sensitive personal data - Information relating to the race, political opinion, religious belief, trade union membership, physical or mental health, sexuality and any criminal history of an individual.

Responsibilities

Responsibilities of Staff – all staff (permanent and temporary)

All staff, whether permanent or temporary, are required to read, understand and accept any policies and procedures that relate to personal data that they may handle in the course of their work.

All staff have a responsibility for data protection and are required to adhere to this Policy, any associated procedures and to attend any associated training.
All staff must:

- Understand the main concepts within the Data Protection legislation; the eight Principles, sensitive data and informed consent.
- Identify and report any risks to the security of personal data processed by the Council to their line manager or the Information Asset Owner.
- Assist their customers/service users to understand their rights and the Council's responsibilities in regards to data protection.
- Identify and report any subject access requests to the Data Protection Officer (DPO) so that they can be processed in accordance with the Data Protection Act.

Temporary staff

It is a requirement of the Council that all temporary staff, agency staff, volunteers, work placement students and all managers requesting access to systems for these temporary workers, should read, and undertake to comply with these guidelines in accordance with the DPA and the Council's Data Protection Policy.

Why users and Managers must follow this Policy

A breach of this policy by a member of staff is likely to lead to disciplinary action being taken. Investigation of any breach of the policy will also include a review of relevant data management procedures.

A breach of the policy by an elected member is a potential breach of the Council's Code of Member Conduct.

If an individual's personal information is disclosed outside its intended purpose, they have a right to sue the person responsible. Individual officers and members of the Council may be prosecuted under the DPA , not just the Council as a whole.

The Computer Misuse Act 1990 (the Act) identifies the legal framework for the definition of and prosecution for unauthorised use or misuse of computers and computer systems. Whilst this Act is particularly intended to deal with unauthorised accesses from outside the organisation ('hackers'), it deals equally with unauthorised accesses from inside. Penalties under the Act fall into two main categories

- Unauthorised access - Anyone gaining access, or attempting to gain access to computer data they are not authorised to see, may face a fine of up to £2,000 or six months in prison, or both; and
- Ulterior intent or unauthorised modification - Anyone accessing data with an ulterior motive, or modifying data without authorisation, may be sentenced to up to five years in prison or an unlimited fine, or both

Security breaches involving personal data can cause harm and distress to the individuals that they affect. Whilst not all security breaches have such consequences, they can still cause serious embarrassment or inconvenience to the people concerned.

Responsibilities of Managers

All managers are required to ensure that they (and their staff) understand and adhere to this Policy and any associated procedures. They are responsible for ensuring that staff are informed and updated on any changes made to this Policy.

All managers must identify and report any risks or breaches to the security of personal data processed by the Council to their relevant line manager or appropriate Information Asset Owner.

All managers must ensure that their staff undertake training in data protection/information security which is specific to their role. Refresher training will be undertaken periodically.

Responsibilities of the Council

As the Council processes personal data on its customers, employees, members, suppliers and members of the public ('data subject') the Council is required to notify the ICO about what information it collects, how it uses that information, who it collects it from and who it shares it with. This process is called the notification. Notifications state what personal date is covered by the notification

To understand more about the Council's obligations as a local authority see the ico.org.uk. https://ico.org.uk/for-organisations/local-government/

For information about the Council's registrations, see the ICO webpage on registrations https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

This Policy applies to personal data processed by Elected Members in their capacity as Councillors and when carrying out their constituency responsibilities. For political activities and campaigning for elections each Elected Member is individually responsible and may need to notify with the ICO personally for these limited purposes.

Privacy Impact Assessment

Before undertaking any work stream, including projects, policies, proposal, initiatives, etc. which is likely to involve personal data the Council will carry out a Privacy Impact Assessment (PIA).

PIA's are a means of addressing project risk as part of overall project management. It is carried out with a view to identifying and managing any project risks relating to personal data which is collected, used, stored, distributed and destroyed throughout a project.

The function of the PIA is to ensure that data protection risks are properly identified and addressed wherever possible, and that decision-makers have been fully informed of the risks and the options available for mitigating them. For those policies that involve data sharing, this could include the risks if data is not shared.

The PIA will set out information such as the personal data to be collected, how it will be used, how it will be stored, whether it will be shared and for how long it will be retained.

Not every proposal will require a PIA. The key questions in determining whether a PIA is needed are:

- Will the proposal involve the processing of personal data of individuals?
- Has a PIA already been conducted?

If personal data will be processed and there is no existing PIA, a PIA should be undertaken.

Data Handling

Collecting and Using Personal Data

Only collect personal data that is necessary. Nothing should be collected on the grounds that it might come in useful. Extra care should be taken when collecting or using sensitive personal data.

When collecting personal data it is important to ensure that the Data Subject is informed who the Data Controller is, the purpose(s) which the personal data is to be used for and any other information about how it will be used or shared.

Personal data must be processed fairly and lawfully. It will be considered to be fairly and lawfully processed if:

- The Data Subject has given their informed consent to the processing.
- The processing is necessary for:
  - The performance of a contract
  - The compliance with any legal obligation of the Data Controller
  - The protection the vital interests of the Data Subject. This means a life or death situation
  - The administration of justice
  - The exercise of any functions conferred on the Council by law
  - For the exercise of any other functions of a public nature exercised in the public interest
  - For the purposes of legitimate interests of the Council or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted.

Personal data should only be used for the purpose(s) for which it is collected and not for any incompatible purpose. If it is to be used for any other purpose then the Data Subject should be advised of the other purpose(s) it is to be used for and the Data Subject consent MUST be obtained.

Anonymisation

Anonymisation is the process of turning data into a form which does not identify individuals and where identification is not likely to take place. This allows for a much wider use of the information. The DPA controls how organisations use 'personal data' – that is, information which allows individuals to be identified. The ICO's 'Anonymisation Code of Practice' explains the issues surrounding the anonymisation of personal data, and the steps an organisation can take to ensure that anonymisation is conducted effectively, while retaining useful data.
https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

Security Classification

Information may be classified into three types: OFFICIAL, SECRET and TOP SECRET. Each attracts a baseline set of security controls providing appropriate protection against typical threats. The majority of information that is received, created, processed, generated, stored or shared within the Council is classed as OFFICIAL additionally; ICT systems and services may require enhanced controls.

Storing personal data – individual duties

It is the responsibility of every employee to ensure that personal data is used and stored properly to prevent any unauthorised access.

Personal data should:

- be stored in locked desks or filing cabinets
- only be accessed and securely protected on Council equipment using industry standards authentication methodologies and limited access
- not be visible on screens by unauthorised persons (including other members of staff)
- not be taken out of the Council offices or stored externally unless such use or storage is necessary and authorised by your line manager
- only be kept for as long as is necessary and disposed of securely when it is no longer needed

Review it regularly and delete it promptly when no longer needed. Archiving personal or sensitive data is still subject to the DPA.

Sensitive personal data should be kept secure and subject to very limited access.

Duplicate records should be kept to a minimum to reduce the risk of unauthorised access or loss and to avoid anomalies.

Disclosing personal data

Personal data should **only** be disclosed in certain circumstances:

Personal information should not be given out to a Data Subject over the telephone unless you have 'no doubts' as their identity and the information is innocuous. For telephone enquiries, check the requested information. If it seems innocuous and the enquirer is able to answer a question from it, take the callers number, call them back and provide the information; but if you have any doubts, ask the caller to put their enquiry in writing and support the information request certified copies of their identifications: Driving Licence or Passport, and a copy of a recent utility bill.

Request by third parties - Staff must take particular care when disclosing personal data to third parties, to ensure that there is no breach of the DPA. Disclosure may be unlawful even if the third party is a family member of the Data Subject, or another local authority or government department. Where a request for disclosure is made by a third party it is important to ensure that you have the Data Subject's written **consent** to the disclosure.

Where the disclosure is required by law, you can forgo consent, however, before any disclosure, the Data Protection Officer should be consulted.

The DPA also allows personal data to be disclosed to third parties without the consent of the data subject, in the following circumstances:

- The disclosure is necessary for safeguarding national security
- The disclosure is necessary to protect the vital interests of the data subject (Data Subject for example to prevent serious harm, or in a life or death situation)
- The disclosure is necessary for the prevention or detection of crime
- The disclosure is necessary for the assessment or collection of any tax or duty

Any request for third party personal information must be in writing (letter or email), stating the legislation under which it is being request and the purpose for which it will be used. It is important that a record who asked for the information, when and why is made.

Whenever data is shared externally, a data sharing agreement must be entered into with the other party or parties', stating what information is to be shared, how it will be shared and how it will be used.

Managers are responsible for ensuring all procedures are correctly followed according to this Policy

Data Subject Access Requests

The DPA provides Data Subjects with the right to find out what information is held by the Council about themselves on computer and paper records.

Data Subjects are entitled to:

- be told if any personal data is held about them by the Council;
- have the information communicated to them in an intelligible and permanent form;
- be told for what purpose(s) the data is processed;
- have explained to them how any automated decisions taken about them were made and if specifically requested the logic involved in making that decision;
- have any reference codes clearly explained to them (where a printout is produced containing personal data)
- be told the recipients to whom the data may have been disclosed.

A formal request from a Data Subject for information that the Council holds about them must be made in writing, preferably by using the request form. A fee of £10.00 is payable by the data subject for provision of this information.
http://www.cotswold.gov.uk/about-the-council/information-data/data-protection/

To help ensure confidentiality, anyone making a subject access request to will be asked to provide the Council with sufficient evidence to confirm their identity e.g. identification pages of passport, a current photo driving licence, a current utility bill, credit card, bank statement any other form of identification which includes their name and address or a certify copy of a Power of Attorney if requesting as such..

The Council shall respond to data subject access request within 40 days. Data subject access request forms are available on the Council website.
http://www.cotswold.gov.uk/media/267102/Data-subject-access-application-form.pdf

Exemptions

There are some special circumstances in which data protection principles are superseded by other concerns. Specific exemptions are set out in Part 4 of and Schedule 7 to, the DPA. There are other exemptions in Regulations made under the DPA. The following are some of the exemptions that often apply:

- Crime and taxation
- Regulatory activity
- Publicly available information
- Disclosures required by law
- Legal advice and proceedings
- Confidential references
- Management information
- Negotiations
- Journalism, literature and art
- Domestic purposes

Breach of Data Protection

If any employee or member of the public becomes aware that there has been a breach of this Policy, they should immediately report it to the Data Protection Officer who will be able to advice on an immediate action to be taken.

Upon receipt of notification of a breach the Data Protection Officer will investigate the allegation and, if substantiated, identify an action plan which will include details of containment and recovery action, an assessment of the risks and identify any notifications that need to take place.

Whilst there is no legal requirement to report serious breaches to the ICO, the Council will undertake an assessment to ascertain if a breach is serious and ought to be reported.

In addition, the Council will consider whether to notify customers. In reaching any decision on whether or not to notify customers or not, the Council will consider the seriousness of the breach, the amount of data, the type of data, the number of customers affected, where the data is now located and whether it is recoverable or not.

Key Messages

- All users **must** be aware of the DPA and the 8 data protection principles.
- Managers are responsible for ensuring users are aware of this Policy and are allowed the time for essential training and any follow up necessary.
- Managers involved in any work streams **must** undertake a Privacy Impact Assessment before any formal decisions are made.
- It is the responsibility of **all users** to ensure they handle data in compliance with this Policy and DPA

- Data subject access requests **must** be dealt with in accordance with the DPA and all time constraints adhered to.
- Any data protection breaches **must** be reported to the Data Protection Officer.
- The Council will assess whether any parties need to be informed, for example the ICO or data subjects.

COTSWOLD DISTRICT COUNCIL

Appendix 1

Do's *and* ***Don'ts*** *of Data Protection*

- Do check that you have consent to share data
- Do check that you have an information sharing agreement in place
- Do think about data as it were about you
- Do only hold data for as long as it is needed
- Do destroy files correctly and confidentially
- Do make sure you have correct and accurate data

- Do not share your passwords
- Do not leave your PC or device unlocked when away from your desk
- Do not leave documents on your desk if they contain personal or sensitive information
- Do not disclose personal information unless you are sure you can and you know who is asking for it