Appendix 'A'

COTSWOLD DISTRICT COUNCIL

COTSWOLD DISTRICT COUNCIL

GENERAL DATA PROTECTION REGULATION POLICY

Contents

Document Control

Version	Date	Author	Comments
1	January 2018	ICT Audit and Compliance Manager	ICO GDPR Compliance

COTSWOLD
DISTRICT COUNCIL

Policy Statement

This Policy describes the Council's requirements to comply with the General Data Protection Regulation (GDPR).

Previously the Data Protection Act 1998 was in place to protect the interest of individuals. The legislation covers both electronic information and manual files the Council holds.

The GDPR requirements were published in the Official Journal of the European Union as Regulation 2016/679 on 27 April 2016. The Regulation will be directly applicable throughout the EU from 25 May 2018, without requiring implementation by the EU Member States through national law.

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

The core themes of the data protection principles in GDPR remain largely as they were in the Directive, though there has been a significant raising of the bar for lawful processing and a new principle of accountability has been added.

The Council must comply with the six (Article 5) principles when collecting or processing personal data:

- Personal data must be processed lawfully, fairly and transparently.
- Personal data can only be collected for a specified purpose.
- Personal data must be accurate, relevant and limited to what is necessary for processing.
- Personal data must be accurate and kept up to date.
- Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.
- Personal data must be processed in a manner that ensures its security.

Scope

This document applies to the following:

- Councillors.
- Committees.
- Services.
- Partners.
- Employees of the Council.
- Contractual third parties and agents of the Council who use ICT facilities, or who require remote access to the Council's Information Systems or information.

This Policy applies to all information which is subject to the GDPR including:

- All personal data which is processed automatically.
- Any personal data held in a manual form in a relevant filing system.
- Personal data held in an accessible record.

This Policy should be applied with appropriate reference to the Council's Information Security policy including, but not restricted to, the following contents within the Policy:

- Access Control.
- Card Payments Standards.
- Email Usage.
- GCSX Acceptable Usage Policy.
- Incident Management.
- Information Protection and Handling Guidance.
- Information Security Standards.
- Equipment Usage.
- Internet Usage.
- Removable Media.
- Reporting of Breaches Procedures.
- Software Security.

Objective

The objective of the GDPR protection policy is to depict the legal data protection aspects in one summarising document. This Policy outlines the Councils legal requirements under the GDPR and the processes for how the Council will meet them.

The Council must comply with all relevant legislation, and maintain good practices to protect the personal data held. It is also required to monitor and review compliance with legislation and introduce changes where appropriate.

This Policy aims to provide 'Lawful bases for processing' which is set out in 'Article 6' of the GDPR. At least one of these must apply whenever the Council processes personal data:

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

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

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.
- Failure to comply with the regulations will lead to significant fines of up to 20 million Euros or 4 percent of the Councils turnover, whichever is higher.
- 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

Automated Decision making - Making a decision solely by automated means without any human involvement.

Biometric Data – Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a person, which allow or confirms the unique identification of that natural person such as facial images. Biometric data is increasingly used as a method of authentication.

Consent – Any freely given, specific, and unambiguous indication of the data subject wishes. It must be a clear affirmative action and a signified agreement for the processing of personal data.

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 information is about.

Data Sharing - The ability to share the same data resource with multiple applications or users. It implies that the data is stored on 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 GDPR requirements.

Genetic data – Personal data relating to the genetic characteristics of a natural person which give unique information about the health or physiology of that person.

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 of one or more assets, by virtue of a managerial position.

Personal data - Information relating to living people who can be identified from that data, or 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.

Profiling - is "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a person, specifically to analyse or predict certain aspects concerning that person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.

Pseudonymisation - Pseudonymisation of data means replacing any identifying characteristics of data with a pseudonym, or a value which does not allow the data subject to be directly identified.

Special Categories data - Personal data which is more sensitive, and requires more protection. This is data relating to the race, political opinion, religious belief, trade union membership, physical or mental health, sexuality and any criminal history of an individual.

Lawful basis for processing

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever the Council process personal data:

- **Consent:** The individual has given clear consent for the Council to process their personal data for a specific purpose:
  - Consent must be fully unbundled from other terms and conditions and will not be valid unless freely given, specific, informed and unambiguous
  - Consent must be as easy to withdraw consent as it is to give – data subjects have the right to withdraw consent at any time.

- **Contract:** This processing is necessary for a contract the Council has with the individual, or because they have asked the Council to take specific steps before entering into a contract. The Council is required to process their personal data to comply with the Councils obligations under the contract.

- **Legal obligation:** A requirement for the Council to comply with the law (not including contractual obligations). Article 6(3) requires that the legal obligation must be laid down by UK or EU law, and confirms that this does not have to be an explicit statutory obligation, as long as the application of the law is foreseeable to those individuals subject to it.

- **Vital interests:** The processing is necessary to protect someone's life. The lawful basis is very limited in its scope, and generally only applies to matters of life and death. It is likely to be particularly relevant for emergency medical care, when the need to process personal data for medical purposes but the individual is incapable of giving consent to the processing.

- **Public task:** The processing is necessary for you to perform a task in the public interest or for Councils official functions.

- **Special Categories:** This is personal data which is more sensitive, and so needs more protection. The data relates to the race, political opinion, religious belief, trade union membership, physical or mental health, sexuality and any criminal history of an individual. The conditions for processing special category data are:

  - With the explicit consent of the data subject.
  - Where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement.
  - Where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent.
  - Limited circumstances by certain not-for-profit bodies.
  - Where processing relates to the personal data which are manifestly made public by the data subject.
  - Where processing is necessary for the establishment, exercise or defence of legal claims.
  - Where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards.
  - Where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services.
  - Where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices.
  - Where necessary for archiving in the public interest, scientific or historical research and statistical purposes.

Rights of an Individual

The GDPR provides the following rights for individuals:

- **The right to be informed**: encompasses our obligation to provide 'fair processing information', through our privacy notice. The processing of personal data will be concise, transparent and easily accessible, written in clear and plain language and free of charge.

- **The right of access**: Individuals can request, in writing to the Data Protection Officer (DPO), to see all personal data held on them, including e-mails or paper files. The Council must fully comply with such requests within 30 days of receipt of the written request. There is no longer a right for controllers to charge a fee, with some narrow exceptions.

- **The right to rectification**: Individuals are entitled to have their personal data rectified if it is inaccurate or incomplete without undue delay.

- **The right to erase**: Also known as 'right to be forgotten'. Individuals have a right to have their personal data erased and to prevent processing in specific circumstances, such as :
  - Where the personal data is no longer necessary in relation to the purpose for which it was originally collected.
  - When the data subject withdraws consent.
  - When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
  - The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
  - The personal data has to be erased in order to comply with a legal obligation.

- **The right to restrict processing**: Individuals have a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested and where the processing is unlawful.

- **The right to data portability**: Data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows Individuals to copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

- **The right to object**: Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest, direct marketing (including profiling) and processing for purposes of scientific/historical research and statistics.

- **Rights in relation to automated decision making and profiling**: GDPR has additional rules to protect individuals if the Council is carrying out solely automated decision-making that has legal or similarly significant effects on them , these rules include:
    - The Council can only carry out this type of decision-making where the decision is necessary for the entry into or performance of a contract.
    - Authorised by Union or Member state law applicable to the controller.
    - Based on the individual's explicit consent.

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 the protection of data 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 GDPR requirements, these include the six principles, 'Lawful basis for processing' and 'Right of an Individual.
- 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 GDPR.
- Identify and report any subject access requests to the Data Protection Officer (DPO) so that they can be processed in accordance with the GDPR requirements.

Temporary staff

It is a requirement of the Council that all volunteers, temporary, agency staff, 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 GDPR requirements and the Council's GDPR 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 this 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 GDPR, 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 access from outside the organisation (hackers), it deals equally with unauthorised access from inside. Penalties under the Act fall into two main categories

- Unauthorised access - Anyone gaining, or attempting to gain access to computer data they are not authorised to see, may face a fine of up to £2,000 and six months in prison.
- 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 and unlimited fine.

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 the 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 the protection of data /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 also applies to personal data processed by Elected Members in their capacity as Councillors and when carrying out their constituency responsibilities. For political activities or when they represent residents of their ward or 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

Privacy Impact Assessment (PIA) is a mandatory requirement for GDPR.
Before undertaking any work stream, including projects, policies, proposal, initiatives, etc. which is likely to involve personal data the Council will carry out a 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 Special categories of data (as per the Lawful bases for processing 'page 6').

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.

Managing data protection risk

Data protection techniques such as 'Anonymisation' and 'Pseudonymisation' assist in reducing the risk of inappropriate disclosure of personal information by the Council whilst

complying with its obligations enabling the Council to make information available to the public and other stakeholders.

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 GDPR 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

Pseudonymisation

Where it is necessary to share personal data but an anonymisation approach is not sufficient to protect the data, then consideration should be given to 'Pseudonymisation' of the data by means replacing any identifying characteristics of the personal data with a pseudonym, or, in other words, a value which does not allow the data subject to be directly identified.

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

Information that is of a particularly sensitive nature is marked OFFICIAL - SENSITIVE. This marking is only be used in limited circumstances primarily when such information is distributed on a "need to know" basis.

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. 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 with 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 GDPR. 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 GDPR 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 of 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 GDPR provides Data Subjects with the 'right' to find out what information is held by the Council about themselves on computer and records, including e-mails or paper files.

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 Councils request form. This information provided is free of charge.
http://www.cotswold.gov.uk/about-the-council/information-data/data-protection/

To help ensure confidentiality and authenticity of the request, 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 or 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 30 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 GDPR principles are superseded by other concerns. 'Article 23' enables Member States to introduce derogations to the GDPR in certain situations.

There are number of exemptions that can be applied from the GDPR's transparency obligations and individual rights, but only where the restriction respects the essence of the individual's fundamental rights and freedoms, the exemptions can fall into the following categories:

- national security;
- defence;
- public security;
- the prevention, investigation, detection or prosecution of criminal offences;
- other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security;

- the protection of judicial independence and proceedings;
- breaches of ethics in regulated professions;
- monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention;
- the protection of the individual, or the rights and freedoms of others; or
- the enforcement of civil law matters.

Breach of Data Protection

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

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.

The GDPR requires all organisations to report certain types of personal data breaches to the ICO. Such as if the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the Council will also inform those individuals without undue delay.

Breaches must be reported to the ICO within 72 hours of the Council becoming aware of the breach, where feasible.

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.

Powers of the Information Commissioner

The following are criminal offences, which could give rise to a fine and/or prison sentence:

- The unlawful obtaining of personal data.
- The unlawful selling of personal data.
- The unlawful disclosure of personal data to unauthorised persons.

Further Information is available at https://ico.org.uk/

COTSWOLD
DISTRICT COUNCIL

Appendix I

***Do's** and **Don'ts** of GDPR*

- 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