information management & security

Gloucestershire COUNTY COUNCIL

Data Protection Policy

1.0 Scope

In order to operate efficiently, Gloucestershire County Council (the council) has to collect and use information about people with whom it works. These include but are not limited to, members of the public, service users, current, past and prospective employees, clients, customers, contractors, suppliers, and partner organisations. In addition, the council may be required by law to collect and use information in order to comply with the requirements of central government.

Personal data must be handled and dealt with properly, no matter how it is collected, recorded, and used, and whether it is on paper, in computer records or recorded by any other means.

The council regards the lawful and correct treatment of personal data as critical to its successful operations, maintaining confidence between the council and those with whom it carries out business. The council will ensure that it treats personal data correctly in accordance with the law.

The council fully endorses and adheres to the principles of data protection as set out in the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR).

This policy applies to all employees, Elected Members, contractors, agents and representatives and temporary staff, working for or on behalf of the council.

This policy applies to all personal data collected, created, or held by the council, in whatever format. For example, paper, electronic, email, microfiche, film and however it is stored, e.g. ICT system/database, SharePoint, OneDrive filing structure, email, filing cabinet, shelving and personal filing drawers.

This policy does not apply to information held by schools. If a request concerns UK GDPR in a school or a wish to access school records, the requester should contact the Head Teacher of the relevant school.

Elected Members should note that they are also data controllers in their own right and are responsible for ensuring any personal data they hold/use in their role as Elected Members is treated in accordance with the UK GDPR.

The UK GDPR does not apply to information about a person if they are deceased.

The DPA 2018 requires the council to maintain an 'appropriate policy document' that sets out how it will protect personal and special category (sensitive) data. This Data Protection Policy and our Special Category Data Protection Policy meets the requirements of Schedule 1 of DPA 2018. The Criminal Convictions Data Policy constitutes the 'appropriate policy document' for personal data relating to criminal convictions. These can be found on our website on our Information Management and Security Policies pages.

2.0 The principles of data protection

The UK GDPR states that anyone processing personal data must comply with **seven principles**. These principles are legally enforceable.

The principles require that personal data:

1. Shall be processed lawfully, fairly, and transparently:
   The council will:
   - ensure that personal data is only processed where a lawful basis applies, and where processing is otherwise lawful.
   - only process personal data fairly and will ensure that data subjects are not misled about the purposes of any processing.
   - ensure that data subjects receive full privacy information (a privacy notice) so that any processing of personal data is transparent.

2. Shall be processed specifically, explicitly, and legitimately:
   The council will:
   - Only collect personal data for specified, explicit and legitimate purposes, and we will inform data subjects what those purposes are in a privacy notice.
   - Not use personal data for purposes that are incompatible with the purposes for which it was collected. If we do use personal data for a new purpose that is compatible, we will inform the data subject first.

3. Shall be adequate, relevant, and not excessive:
   - Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
   - The council will only collect the minimum personal data that we need for the purpose for which it is collected. We will ensure that the data we collect is adequate and relevant.

4. Shall be accurate and kept up to date:
   - The council will ensure that personal data is accurate and kept up to date where necessary. We will take particular care to do this where our use of the personal data has a significant impact on individuals.

5. Shall be kept for no longer than is necessary:
   - The council will only keep personal data in identifiable form as long as is necessary for the purposes for which it is collected, or where we have a legal obligation to do so. Once we no longer need personal data it shall be deleted or rendered permanently anonymous.

6. Shall be processed in a manner that ensures appropriate security, and:
   - The council will ensure that there are appropriate organisational and technical measures in place to protect personal data.

7. The council shall be able to demonstrate compliance with the above.
   The council will:
   - ensure that records are kept of all personal data processing activities, and that these are provided to the Information Commissioner on request.
   - carry out a Data Protection Impact Assessment (DPIA) when legally required and for any high-risk personal data processing, and consult the Information Commissioner if appropriate.
   - ensure that a Data Protection Officer (DPO) is appointed to provide independent advice and monitoring of the council's personal data handling, and that this person has access to report to the highest management level of the council.
   - have in place internal processes to ensure that personal data is only collected, used, or handled in a way that is compliant with data protection law.

The UK GDPR provides conditions for the processing of any personal data that must be met. It also makes a distinction between **personal data, "special category" (sensitive) personal data and criminal conviction personal data** (see glossary for definitions). Special category personal data requires stricter conditions for processing. For guidance on how the council processes special category and criminal conviction personal data please refer to the relevant data protection policies which can be found on our website on our Information Management and Security Policies pages.

3.0 Responsibilities

Gloucestershire County Council is a data controller under the UK GDPR.

The Corporate Leadership Team (CLT) is responsible for ensuring compliance with this policy.

Senior Managers are responsible for ensuring that their business areas have processes and procedures in place that comply with the UK GDPR and this policy. They are responsible for ensuring that data is appropriately protected or that controls are in place to prevent access by unauthorised personnel, and that data cannot be tampered with, lost or damaged. They are also responsible for ensuring that Information Assets have an appropriate nominated owner.

The Data Protection Officer (DPO) is responsible for fulfilling the duties under Article 39 of UK GDPR.

The Information Management Service is responsible for providing day to day advice and guidance to support the council in complying with the UK GDPR and this policy.

Each Information Compliance Champion shall promote good practice and assist their Senior Managers in ensuring compliance with the UK GDPR and this policy. The nomination of such a person shall not release other members of staff from compliance with the UK GDPR and this policy.

Information Asset Owners are responsible for ensuring that the information contained within their systems (paper or electronic) is accessed and shared appropriately and in accordance with the Data Protection Act.

The council appoints Caldicott Guardian/s and Angel/s to provide advice to ensure that where personal data is shared (particularly in relation to patients, children and vulnerable adults) it is done properly, legally and ethically.

All members of staff, contractors and Elected Members who hold or collect personal data are responsible for their own compliance and must ensure that personal and/or special category data is kept and used in accordance with the UK GDPR and this policy. In particular, staff must not attempt to access personal data that they are not authorised to view. Failure to comply with the UK GDPR may result in disciplinary action which could further lead to dismissal and, in some cases, criminal proceedings/ prosecution.

4.0 Related policies

This policy should be read in conjunction with the following policies and procedures:

- Special Category data policy
- Information Rights Policy
- Freedom of Information and Environmental Information Regulations Policy
- Information Security Incident Management Policy
- Information Compliance Internal Review and Complaints Procedure
- Information Security Policy
- Information IT Access Policy

- Information Protection and Handling Standards
- Access to Deceased Person's Records Policy
- Code of Conduct

5.0 Agents, partner organisations and contractors

If a contractor, partner organisation or agent of the council is appointed or engaged to collect, hold, process or deal with personal data on behalf of the council, or if they will do so as part of the services they provide to the council, the lead council officer must ensure that appropriate contractual clauses for security and Data Protection requirements are in place, and that personal data is kept and used in accordance with the principles of the UK GDPR and this policy.

A data confidentiality agreement must be in place prior to a third party being given access to personal data to undertake work that is not under contract, e.g., as part of the tender/procurement process.

6.0 Information / Data sharing

The council may share personal data when it is in the best interests of the data subject and when failure to share information may carry risks to vulnerable groups and/or individuals. This must be done in a secure and appropriate manner. The council will be transparent and as open as possible about how and with whom data is shared; with what authority; and for what purpose; and with what protections and safeguards.

When personal data is shared with other organisations or partners, an information sharing agreement or data sharing agreement must be put in place and signed by all parties. Responsibility and accountability for its implementation lies with the Information Asset Owner. Examples of existing agreements can be found on our Information Sharing page.

When sharing data with a contractor, a contract is required rather than a data sharing agreement. Further detail on data sharing with contractors can be found on our IMS Contracts, Procurements and Projects page on Staffnet.

7.0 Disclosure of personal data about third parties

The personal data of a third party must not be disclosed, except in accordance with the UK GDPR. If you believe it is necessary to disclose information about a third party to a person requesting data, you must first seek advice from the Information Management Service.

8.0 Data quality, integrity, and retention

Personal data must be accurate and where necessary kept up to date. Staff should ensure they are aware of the council's Information and Data Management Strategy and its associated Data Quality Standards.

All staff that are responsible for recording personally identifiable data in council systems should only do so following the completion of appropriate training.

Personal data must not be kept for longer than is necessary, therefore all areas of the council must ensure they have appropriate retention periods in place, and that these are adhered to. These are outlined within the council's Records Retention and Disposal Schedule.

The council will ensure that where special category or criminal convictions personal data is processed:

- there is a record of that processing, and that record will set out, where possible, the envisaged time limits for erasure of the different categories of data.
- that when it is no longer required for the purpose for which it was collected, it will be deleted or rendered permanently anonymous.
- data subjects receive full privacy information (i.e., a privacy notice) about how their data will be handled, where necessary, and that this will include the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

9.0 Data Protection Impact Assessment (DPIA)

The UK GDPR specifically identifies certain situations where a data protection impact assessment is legally required. A DPIA looks at high risk processing and requires Information Asset Owners to assess the necessity, lawfulness, security, and risks of the processing.

All areas of the council must complete a DPIA when utilising:

- Systematic and extensive profiling with significant effects
- Large scale use of sensitive and/or Special Category data
- Public monitoring
- New technologies
- Denial of service (see glossary)
- Large-scale profiling
- Biometrics
- Genetic data
- Data matching
- Invisible processing (see glossary)

- Targeting of children or other vulnerable individuals
- Risk of physical harm

DPIAs must be reviewed by the council's Data Protection Officer (DPO) (dpo@gloucestershire.gov.uk), or a member of the Information Assurance team if the remaining risks are not assessed to be high. They must be kept under review by the service area and the DPO must be updated when there are changes being considered.

The DPO (or member of the Information Assurance Team) must review DPIAs in order to ensure they are aware of the risks of the processing, while the relevant Information Asset Owner must sign off DPIAs in order to ensure an acceptance of associated risks. The Information Management Service will maintain a log of all DPIAs completed.

For more information on DPIAs and how to complete one, visit our Data Protection Impact Assessment page.

10.0 Individual's rights

Refer to the Information Rights Policy for details regarding individual's rights and access to their information. The Information Rights Policy and further supporting procedures can be found on the council's website by visiting the Information Management and Security Policies page. For information on how to exercise these rights, please visit our Information Rights page.

11.0 Complaints

Complaints about how the council processes data under the UK GDPR and responses to subject access requests are dealt with using the council's Information Compliance Complaints Procedure.

12.0 Registration

The UK GDPR requires every data controller processing personal data to register and renew their registration on an annual basis. Failure to do so is a criminal offence. The Information Commissioner maintains a public register of data controllers, on which Gloucestershire County Council is registered.

There are other services within the council that are required to register with the ICO. These include:

- Superintendent Registrar - ZA300297
- Gloucestershire Youth Offending Service - Z6385303

The council's DPO will ensure payments are made on behalf of these services, however each of these needs to be aware of their ICO registration number and confirmation that their annual payment has been made.

The Information Management Service will renew the Data Protection Register annually. Staff and Elected Members should notify the Information Management Service of any change to the processing of personal data so the register can be amended accordingly.

13.0 Breach of policy

Any breach of this policy should be investigated in accordance with the mandatory procedures specified in the Information Security Incident Management Policy. The council will always treat any data breach as a serious issue, potentially warranting a disciplinary investigation. Each incident will be investigated and judged on its individual circumstances, addressed accordingly, and carried out in line with the employee code of conduct.

14.0 Document Control

14.1 Document information

Owner:	Jenny Grodzicka, Head of Information Management Services
Author:	Jenny Grodzicka, Head of Information Management Services
Reviewer:	Zoe Vernon, Information Assurance Officer
Board(s) consulted:	
Date created:	March 2010
Next review date:	October 2027
Approval:	Information Board, September 2020
Date of approval:	
Scheme of Delegation ref:	
Version:	6.4
Classification:	UNCLASSIFIED

14.2 Version History

Version	Version date	Summary of Changes
5-1	June 2016	Updated web links and contact details.
5-2	December 2016	Updated links due to new ICT pages.

Version	Version date	Summary of Changes
5-3	May 2018	Review for UK GDPR. Updated principles. Updated links to new IMS pages. Updated reference to Data Protection Act 2018.
5-4	October 2019	General review. Updated hyperlinks. Amended related policies. Minor formatting changes.
5-5	August 2020	General review. Inserted DPIA requirements. Made amendments and inserted reference to data protection and special category data policies.
6-1	August 2021	General review for website project. Making accessibility changes and updating document.
6-2	December 2022	Accessibility review, updates to formatting and policy titles. Broken links fixed. Section relating to "Disclosure of personal data to a third party policy" removed as out of date.
6-3	June 2024	Removed references to P: and S: drives and replaced with M365 equivalent. Broken links fixed following migration of StaffNet on SP.
6.4	October 2024	Fixed broken links and added extra rows in version control table.

14.3 Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 3 years.

14.4 Contact Us

Post: The Information Management Service
Gloucestershire County Council
Shire Hall
Westgate Street
Gloucester
GL1 2TG

Email: dpo@gloucestershire.gov.uk

Phone: 01452 324000

15.0 Appendices

15.1 Abbreviations & Glossary

Abbreviation	Description
CLT	Corporate Leadership Team
DPO	Data Protection Officer
UK GDPR	UK General Data Protection Regulation
FoIA	Freedom of Information Act 2000
ICT	Information and Communications Technology
SAR	Subject Access Request

Glossary	Description
Caldicott Guardians	Named senior officers in the council who ensure that personal data is processed properly, legally, and ethically.
Criminal Conviction Personal Data	Personal data relating to criminal convictions and offences or related security measures.
Data Controller	The individual or the legal person who controls and is responsible for the keeping and use of personal data on computer or in structured manual files.
Data Subject	The individual who the data or information is about
Denial of service	Decisions about access to a product, service, opportunity or benefit which involves automated decision-making (including profiling) or involves the processing of special category data.
Information Asset Owner	An Information Asset Owner is a member of staff whose seniority is appropriate for the value of the asset they own. Information owners are business managers who operationally own the information contained in their systems (paper and/or electronic). Their role is to understand what information is held, how it is used and transferred, and who has access to it and why, in order for business to be transacted within an acceptable level of risk.
Information Commissioner	The independent person who has responsibility to see that the UK GDPR is complied with. They can give advice on data protection issues and can enforce measures against individuals or organisations who do not comply with the UK GDPR.
Invisible processing	You obtain personal data from somewhere other than directly from the individual themselves, and you don't provide them with the privacy information.
Notified Purposes	The purposes for which the council is entitled to process that data under its notification with the Office of the Information Commissioner.
Personal Data	Defined in s(1) of the UK GDPR, as 'data which relates to a living individual who can be identified from that data, or from

Glossary	Description
	that data and other information which is in the possession of, or is likely to come into the possession of the data controller' (the council is a data controller), and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other in respect of the individual.
Processing	Covers a broad range of activities and is expected that any use of personal data or data by the council will amount to processing.
Processed fairly and lawfully	Data must be processed in accordance with the 3 provisions of the UK GDPR. These are the data protection principles, the rights of the individual, and notification.
Senior Managers	Group Directors, Directors, Lead Commissioners, Operations Leads and Heads of Service
Special Category (sensitive) Data	Information about racial or ethnic origin, sexual life or sexual orientation, biometric and genetic data, religious beliefs (or similar), physical or mental health/condition, membership of a trade union, political opinions or beliefs, details of proceedings in connection with an offence or an alleged offence.
Subject Access Request	An individual's request for personal data under the Data Protection Act 2018.