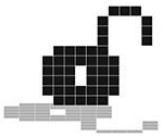

information
management & security

Gloucestershire
COUNTY COUNCIL

Gloucestershire County Council
Data Protection Policy

1. Foreword by the Chief Executive

Information is the life blood of Gloucestershire County Council. Without it, our jobs would be impossible to do.

In order to operate efficiently, we have to collect and use information about people with whom we work. This may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition we may be required by law to collect and use information in order to comply with the requirements of central government.

All personal information 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. We all have a responsibility for its safe handling.

This document sets out the principles of data protection, our responsibilities, the access rights of individuals, information sharing and complaints. I endorse it wholeheartedly.

Pete Bungard
Chief Executive
Gloucestershire County Council

2. Scope

In order to operate efficiently, Gloucestershire County Council (the Council) has to collect and use information about people with whom it works. These may include 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 information 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 information 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 information 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 General Data Protection Regulation (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 information 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, S: and P: drive filing structure, email, filing cabinet, shelving and personal filing drawers.

This policy does not apply to information held by schools. If a request concerns 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 information they hold/use in their role as Members is treated in accordance with the GDPR.

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

3. The principles of data protection

The GDPR stipulates that anyone processing personal data must comply with **six principles** of good practice. These principles are legally enforceable.

The principles require that personal information:

1 Shall be processed lawfully, fairly and transparently;

2 Shall be processed specifically, explicitly and legitimately;

3 Shall be adequate, relevant and not excessive;

4 Shall be accurate and kept up to date;

5 Shall be kept for no longer than is necessary and;

6 Shall be processed in a secure manner

The GDPR provides conditions for the processing of any personal data that must be met. It also makes a distinction between **personal data** and **"special category" (sensitive) personal data** (see glossary for definitions). Special category personal data requires stricter conditions for processing. For guidance on how The Council processes Special category personal data please refer to the Information Rights Policy which can be found here.

4. Responsibilities

Gloucestershire County Council is a data controller under the GDPR.

The Corporate Management Team (CoMT) is responsible for ensuring compliance with this policy. Members of CoMT are responsible for nominating an Information Compliance Champion to promote openness and accountability in their service area.

Senior Managers are responsible for ensuring that their business areas have processes and procedures in place that comply with the 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 Information Management Service is responsible for providing day to day advice and guidance to support the Council in complying with the GDPR and this policy.

Each Information Compliance Champion shall promote good practice and assist their Senior Managers in ensuring compliance with the GDPR and this policy. The nomination of such a person shall not release other members of staff from compliance with the 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 information 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 information is kept and used in accordance with the 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 GDPR may result in disciplinary action which could further lead to dismissal and, in some cases, criminal proceedings/ prosecution.

5. Related policies

This policy should be read in conjunction with the following policies which can be found here

- The Data Subject Rights Policy
- The Subject Access Policy;
- The Freedom of Information and Environmental Information Regulations Policy;
- The Incident Management Policy;
- The Information Compliance Complaints Procedure;
- The Information Security Policy;
- Information IT Access Policy;
- Information Handling Standards;
- Portable Media Policy;
- Remote Working Policy
- Access to Deceased Person's Records Policy
- Code of Conduct

6. 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 GDPR and this policy.

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

7. Information sharing

The Council may share information 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 information is shared with other organisations or partners, a specific information sharing agreement should be put in place and signed by all parties. Responsibility for its implementation lies with the Information Asset Owner. Examples of existing agreements can be found at http://www.gloucestershire.gov.uk/council-and-democracy/data-protection/information-sharing/

Further detail is provided in 'Guidance - Information Management and Security in Commissioning and Partnerships' which is available at https://staffnet.gloucestershire.gov.uk/internal-services/information-management-service/information-management-and-security-in-contracts/

8. Disclosure of personal information about third parties

The personal data of a third party must not be disclosed, except in accordance with the 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.

9. Disclosure of personal information to a third party

See Disclosure of Personal Information to Third Parties Policy for details regarding when/if it is appropriate to share personal data with a third party.

10. 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 Data Quality Strategy and its associated Data Quality standards.

All staff that responsible for recording person-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 schedules in place, and that these are adhered to.

11. 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 at http://www.gloucestershire.gov.uk/council-and-democracy/data-protection/requesting-access-to-your-personal-information/

12. Complaints

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

13. Notification

The GDPR requires every data controller processing personal data to notify and renew their notification 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.

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.

14. Breach of policy

Any breach of this policy should be investigated in accordance with the mandatory procedures specified in the 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.

15. Review of policy

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

16. Contacting the Information Management Service

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

Via Email:
dpo@gloucestershire.gov.uk
Phone: 01452 32 4000

17. Abbreviations

Abbreviation	Description
CoMT	Corporate Management Team
GDPR	Data Protection Act 2018
FoIA	Freedom of Information Act 2000
ICT	Information and Communications Technology
SAR	Subject Access Request

18. Glossary

Caldicott Guardians	Named senior officers in the Council who ensure that personal information is processed properly, legally and ethically.
Data Controller	The individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files.
Data Subject	The individual who the data or information is about
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 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 GDPR.
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 GDPR, as 'data which relates to a living individual 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' (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 information 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 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.

19. Document information

Owner:	Jane Burns, Director Strategy & Challenge
Author:	Jenny Grodzicka, Corporate Information & Compliance Manager
Last Reviewer:	Pete Moore, Information Security Adviser
Create Date:	March 2010
Next review date:	April 2021
Approval:	Information Board, 10 July 2015
Equalities Impact Assessment	Initial screening, Jan 2010
Version:	5-3
Classification:	**UNCLASSIFIED**

20. 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.
5-3	May 2018	Review for GDPR. Updated principles. Updated links to new IMS pages. Updated reference to Data Protection Act 2018.