information management & security

Gloucestershire COUNTY COUNCIL

Information Rights Policy

1.0 Policy Statement

Under the General Data Protection Regulation (GDPR), an individual has a number of rights over the information held about them by any organisation.

Gloucestershire County Council (the council) will ensure that these rights can be fully exercised by everyone. In order to operate efficiently, we collect and use information about the people we work with. This may include members of the public, current, past and prospective employees, service users, customers, and suppliers.

2.0 Scope

This policy covers the rights attributed to data subjects by the GDPR and the Data Protection Act (DPA) 2018. The data subject [you] is the person whose personal data are collected, held or otherwise processed.

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

3.0 Responsibilities

The council is a data controller under GDPR.

The Corporate Leadership Team (CLT) is responsible for ensuring compliance with this policy. Members of CLT 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 up to date privacy notices, processes and procedures in place that comply with the GDPR, DPA 2018 and this policy.

Senior managers are responsible for ensuring that, when rights requests are made directly to contracted providers or agents who are processing personal data and providing services on behalf of the council, they are forwarded onto the council.

Providers are also expected to support the council in responding to these rights request, in line with their responsibilities under GDPR.

The Information Management Service (IMS) will centrally manage the process of handling information rights requests and will liaise with relevant service area contacts to determine how to respond to the request.

A central register of privacy notices will be maintained by IMS and can be viewed on our Service specific Privacy notices page

IMS is responsible for providing day to day advice and guidance to support the council in complying with the DPA 2018 and this policy.

IMS is responsible for drawing up guidance on data subject rights and promoting compliance with this policy, to ensure the easy, appropriate and timely response to requests.

IMS is responsible for monitoring and reporting to Audit & Governance Committee on responses to information rights requests.

All staff are responsible for:

- completing new starter and annual refresher training;
- identifying and reporting requests to IMS without delay; and
- ensuring that any support required to action a request is completed within agreed timescales.

4.0 Timescales

We will provide you with a response within one month of receiving a request, relevant identification, consent (where appropriate) and sufficient details to locate the required information.

In some circumstances we can extend this timescale by a further two months, if the request is complex or numerous. If we extend this timescale we will inform you of the extension within one month of receipt of the request, together with the reasons for the delay.

5.0 Fees

We do not generally charge for responding to these rights.

However, we can charge a reasonable fee or refuse to respond to requests where they are excessive, repetitive or until a reasonable period has elapsed since responding to the last request (Article 12 of the GDPR); we have defined that period as 12 months.

6.0 Individuals' Rights

6.1 Right to be informed

You have the right to be informed about the collection and use of you personal data. We provide this information in the form of Privacy Notices.

6.2 Right of access

You may request a copy of any data held about you, or information about the reasons for which it is kept and processed; known as a Subject Access Request. The request can be made verbally or in writing.

The information held within files can hold many answers to a person's past, and we recognise the positive importance of accessing files, especially when they may be the only source of information regarding someone's childhood and family. All individuals have a right of access to both current open files and closed files relating to their past, e.g. post-care adults (adults who were in the council's care as children).

If you are in receipt of council services we aim to be open and share information with you. Where this is not possible requests will be handled in accordance with our supporting procedures, which can be found on our website at Access my personal information.

Extension to timescales: The one month timescale can be extended by a further two months, if the request is complex.

Exceptions:

- We will only withhold information if there is a legal reason to do so.
- If the personal data is unstructured (i.e. not filed by reference to the data subject) we will refuse requests where it would exceed the appropriate limit (e.g. 18 hours of work) to locate, retrieve and extract the information.
- We may also refuse requests where they are excessive, repetitive or until a reasonable period has elapsed since responding to the last request (Article 12 of the GDPR); we have defined that period as 12 months.
- You will not be able to access information about other people without their consent.
- Where the information is about a child we will follow the process set out in the subject access supporting procedures, which can be found on our website at Access my personal information.

6.3 Right to rectification

You are entitled to have personal data rectified (corrected) if it is inaccurate or incomplete. If we have disclosed the personal data in question to others, we will contact each recipient and inform them of the rectification, unless this proves

impossible or involves disproportionate effort. If asked to, we will also inform you about these recipients.

The nature of the council's work means that we may record opinions as part of an individual's record. In line with ICO guidance, we will ensure it is clear if an opinion is being recorded and whose opinion it is. If it becomes apparent that the opinion is based on inaccurate data, this will be made clear on the record to ensure it is not misleading, but it is unlikely that we will change a recorded professional opinion. Where it is found that there has been an error in recording on an individual's record, wherever possible we will correct the mistake. However, there may be circumstances where we need to keep a record of the error and any action taken as a result of it, but if this is the case we would explain the reasons to you.

6.4 Right to erasure (right to be forgotten)

You have the right to request the deletion or removal of personal data we hold about you.

When the right applies:

- We no longer need to use the personal data for the purposes we collected it for;
- You withdraw your consent from using the personal data where you provided it;
- You object to the use of the personal data and there are no overriding legitimate grounds for us to continue using it;
- We use the personal data unlawfully; or,
- We are legally obliged to erase the personal data.

Exceptions:

The right does not provide an absolute 'right to be forgotten'. There are some specific circumstances where the right to erasure does not apply. We can refuse to comply with a request for the following reasons:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
- For public health purposes in the public interest;
- Archiving purposes in the public interest, scientific research, historical research or statistical purposes; or,
- The exercise of legal claims.

6.5 Right to restriction of processing

You have the right to restrict the processing of personal data. The right applies when;

- You contest the accuracy of the personal data;

- The data has been unlawfully processed;
- We only need to keep the personal data in order to establish or defend a legal claim; or,
- You have successfully objected to the processing and we are determining what legitimate grounds override your objections.

If the information in question has been disclosed to others we will contact each recipient and inform them of the restriction on processing of the personal data, unless this proves impossible or involves disproportionate effort. If asked to, we will also inform you about these recipients.

We would then no longer be able to process that specific personal data for any reason beyond storing it.

We will inform you when we decide to lift a restriction on processing.

6.6 Right to data portability

The right to data portability allows you to obtain and reuse your personal data for your own purposes across different services. It allows you to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

When the right applies:

- to personal data you have provided to a controller;
- where the processing is based on the your consent or for the performance of a contract; and
- when processing is carried out by automated means.

Exceptions:

- This right does not apply to information that we have collected due to a legal obligation or is performance of a public task or statutory responsibility that we have.

6.7 Right to object

When the right applies:

You have the right to object to the processing of your personal data when it is based on:

- the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

You must have an objection on “grounds relating to your particular situation”.

Exceptions: We will stop processing the personal data unless:

- we can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

We will advise individuals of their right to object “at the point of first communication” and in our privacy notices.

6.8 Automated individual decision making and profiling

Where we use automated decision making and profiling of individuals (without any human involvement), we shall ensure that;

- the processing is necessary for the entry into or performance of contract; or
- it is authorised by Union or Member state law applicable to the controller; or
- it is based on the individual’s explicit consent.

We will make sure that when this type of processing occurs, we will:

- give individuals information about the processing;
- introduce simple ways for them to request human intervention or challenge a decision;
- carry out regular checks to make sure that our systems are working as intended.

7.0 What if we refuse your request?

Where we determine that no action is to be taken the council will explain to you why we have refused your request, inform you of your right to appeal to the Information Commissioner’s Office and the possibility of seeking a judicial remedy.

8.0 How to use these Rights

If you wish to use these rights on some or all of your personal data held by the council, then you should contact the council:

Online: My information rights

In Writing:

Information Management Service
Gloucestershire County Council
First Floor, Block 4(a)
Shire Hall, Westgate Street
Gloucester
GL1 2TG

Email: Managemyrequests@gloucestershire.gov.uk

9.0 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

10.0 Appeals

We will inform you of your relevant right to appeal to the Information Commissioner's Office and/or to take legal action when responding to your request.

11.0 Document Control

11.1 Document information

Owner:	Jenny Grodzicka, Head of Information Management Services (DPO)
Author:	Nick Holland, Information Governance Specialist (GDPR) Pete Moore, Information Governance Officer (Security)
Last Reviewer:	Zoe Vernon, Information Assurance Support Officer
Date created:	March 2018
Next review date:	September 2022
Approval:	Information Board, November 2021 (v1.2)
Version:	1.3
Classification:	UNCLASSIFIED

11.2 Version History

Version	Version date	Summary of Changes
0.1	April 2018	Draft policy
1	May 2018	Published Policy
1.1	July 2019	Minor revisions to bring policy in line with the latest ICO guidance and to ensure consistency with other associated council policies
1.2	September 2021	Accessibility updates. Approved at Information Board, 11th November 2021.
1.3	December 2022	Accessibility review and updates to formatting. Broken links fixed.

11.3 Review

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

11.4 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

Appendices

Appendix A - Abbreviations & Glossary

Abbreviation	Description
CLT	Corporate Leadership Team
DPA	Data Protection Act 2018
FoIA	Freedom of Information Act 2000
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
SAR	Subject Access Request

Glossary	Description
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 Protection Officer	The DPO is a statutory role that assists organisations with monitoring internal compliance, informs and advises on data protection obligations, provides advice regarding Data Protection Impact Assessments (DPIAs) and acts as a contact point for data subjects and the supervisory authority.
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's Office	The supervisory authority that has responsibility to see that the GDPR and DPA 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	The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.
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.

Glossary	Description
Senior Managers	Group Directors, Directors, Lead Commissioners, Operations Leads and Heads of Service.
Sensitive (Special Category) 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 GDPR.

Appendix B - Related Policies

- Data Protection Policy
- Freedom of Information Policy
- Information Security Policy
- Access to Deceased Records Policy

Appendix C - Legal context

General Data Protection Regulation (GDPR)

Set outs the rights that individuals have over the use of their personal data.

Data Protection Act 2018 (DPA)

Extends the rights of individuals to cover the processing of personal data for law enforcement purposes.

Freedom of Information Act 2000 (FOI)

This Act extended some of the provisions of the Data Protection Act to unstructured information held by public authorities. It also made it a criminal offence to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of information when a request has been made.

The Adoption and Children Act 2002

This Act restates and amends the law relating to adoption, and access to information which would enable an individual to obtain a certified copy of their birth records.

The Pupil Information Regulations 2005

These regulations provide the right of access to educational records. This includes any statement of special educational needs and educational psychology assessments.

The Access to Health Records Act 1990

Rights of access to deceased patient health records by specified persons. For guidance on accessing deceased patient health records please see (Access to deceased records policy hyperlink).