information management & security

Gloucestershire COUNTY COUNCIL

# Special Category Data Policy

## 1. Policy Statement

This policy sets out Gloucestershire County Council's (the council) processing of special categories of personal data (special category data). It is intended to guide council staff in what to consider when processing this data and how to meet the requirements set out in data protection legislation.

This policy also serves as the Appropriate Policy Document for Special Category Data as required by Schedule 1, Part 4 of the Data Protection Act (DPA) 2018. The policy document explains;

- The council's procedures for ensuring compliance with the principles in Article 5 of the UK General Data Protection Regulation (UK GDPR) when processing Special Category Data, and,
- Where the council's policies on the retention and erasure of special category data and Record of Processing Activities (ROPA) can be found.

All members and officers of the council should be aware of this policy and in particular the safeguards set out in Section 6. Service Leads and Information Asset Owners (IAOs) should engage with the Information Management Service (IMS) where their services process special category data.

## 2. What is Special Category Data

Article 9 of the UK GDPR sets out that special category data consists of personal data that includes:

- Racial or ethnic origin,
- Political opinions,
- Religious or philosophical beliefs,
- Trade Union membership,
- Genetic data,
- Biometric data for the purpose of identifying an individual,
- Health or data about an individual's physical or mental condition,
- Data concerning a person's sex life or sexual orientation.



Information Management Service
Date: July2022
Version: 1-2
Email:dpo@gloucestershire.gov.uk
Telephone: 01452 324000

Special category data does not include personal data relating to criminal convictions and offences, this information is treated differently under data protection legislation. For further information, please see the council's Criminal Conviction Data Policy.

## 3. What the legislation says

Article 9(1) of the UK GDPR states that processing of special category data is prohibited, unless a specific condition from Article 9(2) can be met.

These conditions are:

| | |
|---|---|
| 9(2)(a) | The data subject has given explicit consent to the processing, |
| 9(2)(b) | Processing is necessary in the field of employment and social security and social protection law |
| 9(2)(c) | Processing is necessary in order to protect vital interests of the data subject or another data subject |
| 9(2)(d) | Processing is necessary for the legitimate activities of a not-for-profit body |
| 9(2)(e) | Processing relates to personal data which are manifestly made public by the data subject |
| 9(2)(f) | Processing is necessary for legal claims |
| 9(2)(g) | Processing is necessary for reasons of substantial public interest |
| 9(2)(h) | Processing is necessary for the provision and/or management of health and/or social care systems |
| 9(2)(i) | Processing is necessary for reasons of public interest in the area of public health |
| 9(2)(j) | Processing is necessary for archiving purposes in the public interest |

Sections 10(1-3) of the DPA 2018 makes it clear that where conditions

- 9(2)(b) (employment, social security and social protection),
- 9(2)(h) (health and social care),
- 9(2)(i) (public health), and
- 9(2)(j) (archiving, research and statistics),

are relied upon then **a condition from Part 1 of Schedule 1 of DPA 2018** must also be met.

If condition

- 9(2)(g) (substantial public interest)

is relied upon then **a condition from Part 2 of Schedule 1** must also be met.

## 4. Meeting a Schedule 1 condition

Parts 1 and 2 of Schedule 1 of DPA 2018 provide a number of separate conditions to meet the requirement set out by Section 10. Below are examples of where the

council processes special category data and the Schedule 1 conditions that are most appropriate for that processing.

***Note: These conditions only cover the lawfulness aspect of the first principle. Any processing of personal data using one of these conditions should still consider the fairness, transparency, adequacy and security of the processing.***

| **Example:** | **Schedule 1, Part 1 or 2 condition(s):** |
|---|---|
| Recruitment; undertaking pre-employment checks; HR investigations; change in personal circumstances | **Part 1(1)(1)(a)** – with obligations in connection with employment, or;<br>**Part 2(6)(2)(a)** – the exercise of a function conferred on a person by an enactment |
| Adult and Children Social care and/or Safeguarding | **Part 1(1)(1)(a)** – with obligations in connection with social security or social protection, or;<br>**Part 1(2)(1)** – necessary for health or social care purposes, or;<br>**Part 2(6)(2)(a)** – the exercise of a function conferred on a person by an enactment; or;<br>**Part 2(18)(a)** – necessary for the purposes of protecting an individual from neglect or physical, mental or emotional harm. |
| Equalities Monitoring | **Part 2(8)** – necessary for the purposes of equality of opportunity, or;<br>**Part 2(9)** – necessary for the purposes of promoting or maintaining diversity in the racial and ethnic origins of individuals who hold senior positions in the organisation, or;<br>**Part 2(6)(2)(a)** – the exercise of a function conferred on a person by an enactment. |
| Public Health | **Part 1(2)(1)** – necessary for health or social care purposes, or;<br>**Part 1(3)** – necessary for the reasons of public interest in the area of public health, or;<br>**Part 2(6)(2)(a)** – the exercise of a function conferred on a person by an enactment. |
| Community safety and functions in respect of crime and disorder | **Part 2(10)(a)** – necessary for the purposes of the prevention of detection of an unlawful act, or;<br>**Part 2(6)(2)(a)** – the exercise of a function conferred on a person by an enactment |
| Disclosure to elected representatives responding to requests from constituents | **Part 2(24)** – the processing consists of the disclosure of personal data to an elected representative or person acting under their authority. |

| Example: | Schedule 1, Part 1 or 2 condition(s): |
|---|---|
| Disclosure as part of a Data Subject Access request. | **Part 2(6)(2)(a)** – the exercise of a function conferred on a person by an enactment. |
| Archiving, statistical or historical research | **Part 1(4)** – necessary for archiving, statistical or historical research purposes that are in the public interest (and in accordance with Article 89) |
| Preventing fraud or disclosing information to an anti-fraud organisation | **Part 2(14)(a)** – necessary for the purposes of preventing fraud or a particular kind of fraud. |
| Disclosure as part of a request from the Police or another authority to support with investigations | **Part 2(10)(a)** – necessary for the purposes of the prevention of detection of an unlawful act, or; **Part 2(6)(2)(a)** – the exercise of a function conferred on a person by an enactment |

# 5. Appropriate Policy Document and Additional Safeguards

Schedule 1, Part 4, of the DPA 2018 requires the council to create and maintain an Appropriate Policy Document and keep a Record of Processing Activities in relation to processing of special category data.

## 5.1 Appropriate Policy Document

The following statements explain how the council meets the requirements of the Principles from Article 5 of the UK GDPR in connection with the processing of special category data.

**Principle 1 – Lawful, fair and transparent**

The council will;

- Ensure that special category data is only processed where a lawful basis applies.
- Ensure that processing does not take place unless the reason for processing is derived from a lawful basis from Article 9 of the UK GDPR (see Section 3) and if necessary a Schedule 1 condition from DPA 2018 (see Section 4). and it does not infringe data protection legislation or any other law.
- Only process personal data fairly and ensure that data subjects are not misled about the purposes of any processing.
- Ensure that data subjects receive full privacy information about the processing, unless an exemption applies.
- Complete a Data Protection Impact Assessment (DPIA) for any high-risk processing involving the use of special category data. The assessment should be completed by the relevant Information Asset Owner (IAO).

**Principle 2 – Purpose limitation**
The council will:

- Only process personal data for specific and explicit purposes which will be included within the relevant Privacy Notice, unless an exemption applies.
- Not use personal data for purposes that are incompatible with the purposes for which it was collected, unless required by law. The council will inform data subjects of this change unless a relevant exemption applies or is required by law not to disclose the new purpose.
- Where a council service wishes to use personal data for a different purpose, they should consult IMS for advice.

**Principle 3 – Data minimisation**
The council will ensure that special category data processed by the council shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

**Principle 4 – Accuracy**
The council will:

- Ensure that special category data is accurate and where necessary kept up to date.
- Ensure that data quality is maintained in line with the council's Data Quality Standards.
- Ensure personal data based on a personal assessment and opinion (including intelligence) is distinguished from that which is based on fact.

**Principle 5 – Storage Limitation**
All special category data will be retained in accordance with the council's Records Retention and Disposal Schedule.

**Principle 6 – Security**
Special category data must be protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. The council's Information Security Policy sets out the security requirements internally, and the Cyber and Information Management (Procurement) Policy sets out the security requirements for third party suppliers (processors).

The council has a wide range of technical and procedural controls in place, in order to protect the Special Category Data it processes. These controls are overseen by the council's Information Board and the Senior Information Risk Owner (SIRO), supported by a network of IAOs.

These controls include, but are not limited to;

- Mandatory information security training for all staff.
- Mandatory acceptance of Data Protection, Information Security and IT Access policies by all staff.
- Encryption of data in transit (i.e. secure email) where appropriate.

- Appropriate levels of encryption, firewalls, and business continuity arrangements for corporately servers holding personal data. Council hosted systems are located in the UK and accredited to ISO 27001.
- Contracts with processors and suppliers that contain appropriate UK GDPR and data protection clauses.
- Controlled access for systems holding special category data.
- Corporately backed data protection by design processes and culture to ensure information security has been considered and implemented, via Data Protection Impact Assessment where appropriate, prior to the processing of personal data.
- ID badges to control access to council buildings, which is reinforced by controls to confirm authenticity of badges by machine and by staff.
- An established Information Security incident procedure, in order to mitigate risk and ensure the council complies with its legal obligations where potential breaches may have occurred.

**Principle 7 – Accountability**
The council must be responsible for and demonstrate compliance with these principles. The council will:

- Ensure that records are kept of all processing activities involving special category data (see section 6.5 below).
- Ensure that IAOs will complete a Data Protection Impact Assessment for any high-risk processing involving the use of special category data.

The council has appointed a Data Protection Officer whose role is to provide independent advice on data protection to the council, and to monitor compliance with relevant Data Protection legislation.

## 5.2 Retention of Appropriate Policy Document

- The policy document will be retained for the length of the processing of special category data plus six months.
- The council will review the policy on an annual basis, as per Information Commissioner's Office (ICO) guidance.
- The council will make the policy available to the ICO upon request and without charge.

## 5.3 Record of Processing

The council maintains a Record of Processing Activities via the Information Asset Register (IAR). The information within the ROPA includes

- Which processing condition of Schedule 1, Parts 1 to 2 are relied upon,
- How the processing satisfies Articles 6 and 9 of the UK GDPR, and
- The retention periods for data.

IAOs and Information Asset Managers are provided with access to the IAR by the Information Management Service. IAOs are accountable for ensuring that the Information Asset Register is kept accurate and up to date.

### 5.4 Data Subject Rights

Details of individual's rights and how they access their information can be found in the Information Rights Policy , along with further supporting procedures this can be found on the council's website.

## 6 Agents, partners organisations and contractors

If a contractor, partner organisation or agent of the council is appointed or engaged to collect, hold, process or deal with special category 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 for that service must ensure that appropriate contractual clauses for security and data protection requirements are in place. Personal data must be processed in accordance with the principles of data protection law and this policy.

## 7 Further information

For further information or specific guidance please visit the IMS pages on Staffnet or contact dpo@gloucestershire.gov.uk.

## 8 Related polices

When reading this policy consideration must also be made to the below policies and guidance, which are available on the council website;

- Data Protection Policy
- Information Security Policy
- Criminal Conviction Data Policy
- Information Management Principles
- Internet and Digital Communications Policy
- Information Rights Policy
- Information Sharing guidance
- Information and Records Management Policy
- Records Retention and Disposal Schedule
- Data Quality Standards

# 9 Document information and review

| | |
|---|---|
| **Owner:** | Jenny Grodzicka, Head of Information Management (DPO) |
| **Author:** | Nick Holland, Senior Information Governance Adviser |
| **Last Reviewer:** | Alice Huggins |
| **Date created:** | June 2020 |
| **Next review date:** | July 2023 |
| **Approval:** | Information Board, 15 September 2020 |
| **Version:** | 1 |
| **Classification:** | **UNCLASSIFIED** |

## Version History

| Version | Version date | Summary of Changes |
|---|---|---|
| 1 | June 2020 | First version |
| 1.1 | Sept 2021 | Reviewed in line with policy review aims |
| 1.2 | July 2022 | Accessibility check and replaced broken links |

# Appendices

## Appendix 1 Abbreviations & Glossary

| Abbreviation | Description |
|---|---|
| IMS | Information Management Service |
| IAO | Information Asset Owner |
| ICO | Information Commissioner's Office |
| DPA | Data Protection Act 2018 |
| FoIA | Freedom of Information Act 2000 |
| UK GDPR | United Kingdom General Data Protection Regulation |
| LED | Law Enforcement Directive |
| SAR | Subject Access Request |

| Glossary | Description |
|---|---|
| **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 (DPO)** | 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 personal data or information is about |
| **Information Asset Owner (IAO)** | 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 (ICO)** | The supervisory authority who has responsibility to see that the UK 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 UK GDPR. |
| **Personal Data** | The UK 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 involving personal data, such as collecting, storing, reviewing, editing, deleting, sharing and |

| | |
|---|---|
| | permanent preservation. It is expected that any use of personal information or data by the Council will amount to processing. |
| **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 (SAR)** | An individual's request for personal data under the UK GDPR. |