information management & security

Gloucestershire COUNTY COUNCIL

Criminal Conviction Data Policy

1. Policy Statement

This policy sets out Gloucestershire County Council's (the council) processing of personal data relating to criminal convictions and offences (henceforth Criminal Conviction Data). It is intended to guide council staff in what to consider when processing Criminal Conviction Data and how to meet the requirements set out in Data Protection Legislation.

This policy also serves as the Appropriate Policy Document for Criminal Conviction 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 General Data Protection Regulation (GDPR) when processing of Criminal Conviction Data, and,
- Where the council's policies on the retention and erasure of Criminal Conviction 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 Criminal Conviction Data.

2. What is Criminal Conviction Data

Chapter 2, Part 2, Section 11 of the DPA 2018 states that "personal data relating to criminal convictions and offences or related security measures include personal data relating to:

(2)(a) The alleged commission of offences by the data subject, or;

(2)(b) Proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing."

Criminal Conviction Data may exist as a record in its own right, or it may form part of a larger record that contains other types of personal or special category data.

The council has interpreted the definition of (2)(a) as being met where:

Information Management Service
Date: June 2020
Version: 1-0
Email:dpo@gloucestershire.gov.uk
Telephone: 01452 324000

- the allegation would result in the council reporting the individual to a relevant authority,
- where the police or another authority have advised us of alleged criminal offences and convictions, or
- where the council has power to carry out an investigation itself.

3. What the legislation says

In order to comply with the GDPR when processing Criminal Conviction Data the council must have a lawful basis under Article 6(1) and either legal or official authority for the processing under Article 10.

Article 10 states;

> "Processing of personal data relating to criminal convictions and offences or security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority."

This means that the council must either:

- Process the data in an official capacity; or
- Meet a specific condition in Schedule 1 of the DPA 2018, and comply with the additional safeguards (Schedule 1, Part 4) set out in that Act.

Note: Even if the council has a condition for processing offence data, the council can only keep a comprehensive register of criminal convictions if it does so in an Official Capacity.

The Law Enforcement Directive (LED), enacted in the UK as Part 3 of the DPA 2018, covers the processing of Criminal Conviction Data by Competent Authorities, which is defined as;

> "Any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".

4. Processing in an Official Capacity or as a Competent Authority

As per Section 8 of the DPA 2018, the council is deemed to be working in an Official Capacity or Official Authority when processing personal data that is necessary for the exercise of a function conferred on it by an enactment or activity. Official

Authority can also include council powers that are not necessarily set out in legislation, such as our powers as a Highway Authority, the Fire and Rescue Authority or the Trading Standards Authority.

In relation to the LED, the council would be considered a Competent Authority where processing data as part of its Trading Standards functions. Any processing carried out by a Competent Authority which is **not for the primary purpose of law enforcement** will be covered by the general processing regime under part 2 of the DPA 2018.

The table below details which legislation applies to each type of processing:

Processing Activity	**Legislation**
Where the council is acting as a competent authority	Part 3 and Schedule 8, DPA 2018 (LED)
Where the council is not acting as a competent authority, but the information relates to a criminal offence	Parts 1, 2, and 3 of Schedule 1, DPA 2018
Where the information relates to civil offences	GDPR

5. Meeting a Schedule 1 condition

Where an organisation doesn't have Official Capacity it must meet a specific condition in Schedule 1 of the DPA 2018. Parts 1 to 3 of that schedule provide a number of conditions. Below are examples of where the council processes Criminal Conviction 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 and adequacy of the processing.

Example:	**Schedule 1, Part 1, 2 or 3 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; **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; **Part 1(2)(1)** – necessary for health or social care purposes, or; **Part 2(6)(2)(a)** – the exercise of a function conferred on a person by an enactment; or **Part 2(18)(a)** – necessary for the purposes of

Example:	Schedule 1, Part 1, 2 or 3 condition(s):
	protecting an individual from neglect or physical, mental or emotional harm.
Trading Standards; Licensing; meeting legislative requirements for responding to unlawful acts	**Part 2(12)** – necessary for the purposes of complying with a regulatory requirement which involves establishing whether a person has committed an unlawful act or been involved in dishonesty, malpractice or other seriously improper conduct; **Part 2(11)** – necessary for the exercise of a protective function in protecting/ the public against dishonesty, malpractice or other seriously improper conduct
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)
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; **Part 2(6)(2)(a)** – the exercise of a function conferred on a person by an enactment (depending on whether the council has official authority).
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 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.
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.
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

6. 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 Criminal Conviction Data.

6.1 Appropriate Policy Document

The following statements explain how the council meets the requirements of the Principles from Article 5 of the GDPR in connection with the processing of Criminal Conviction Data.

Principle 1 – Lawful, fair and transparent

The council will;

- Ensure that Criminal Conviction Data is only processed where a lawful basis applies.
- Ensure that processing does not take place unless the reason for processing is derived from legal powers granted to the council 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 Criminal Conviction 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. We will inform data subjects of this change unless a relevant exemption applies or 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 Criminal Conviction 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 Criminal Conviction 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 that a distinction between the data relating to the below categories of data subjects is made;
    - Suspects,

  - Those convicted of criminal offences,
  - Victims, and
  - Witnesses or individuals with information about offences.
- Personal data based on a personal assessment and opinion (including intelligence) must be distinguished from that which is based on fact.

Principle 5 – Storage Limitation

All criminal conviction data will be retained in accordance with the council's Records Retention and Disposal Schedule.

Principle 6 – Security

Information processed for a law enforcement purpose 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 criminal conviction 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 GDPR and data protection clauses.
- Role based access for systems holding Criminal Conviction 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 Criminal Conviction 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 Criminal Conviction 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.

6.2 Retention of Appropriate Policy Document

- The policy document will be retained for the length of the processing of Criminal Conviction 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.

6.3 Record of Processing

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

- Which processing condition of Schedule 1, Parts 1 to 3 are relied upon,
- How the processing satisfies Article 6 of 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.

6.4 Data Subject 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.

7. 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 Criminal Conviction 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.

8. Further information

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

9. 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
- 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

10. Document information and review

Owner:	Jenny Grodzicka, Head of Information Management (DPO)
Author:	Nick Holland, Senior Information Governance Adviser
Last Reviewer:	
Date created:	June 2020
Next review date:	June 2021
Approval:	Information Board, 19th June 2020
Version:	1
Classification:	**UNCLASSIFIED**

Version History

Version	Version date	Summary of Changes
1	June 2020	First version

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
GDPR	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 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.
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 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 GDPR.