Gloucestershire Constabulary Appropriate Policy Document
Sensitive Processing for Law Enforcement Purposes

Gloucestershire Constabulary (GC) is a police force established under the Police Act 1996. The Data Protection Team can be contacted at:

Gloucestershire Constabulary Police Headquarters, No 1 Waterwells, Waterwells Drive, Quedgeley, Glos GL2 2AN

Data.ProtectionOffice@gloucestershire.pnn.police.uk

What this Policy does

This policy explains GC procedures for securing compliance with the data protection principles listed below in relation to sensitive processing for law enforcement purposes. It also explains the retention and erasure policies in relation to the sensitive processing. This policy is a requirement under section 42 of the Data Protection Act 2018 (DPA).

What is sensitive processing?

Sensitive processing is defined in Section 35(8) of the Act and means the processing of personal data of:

- Racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership.
- Genetic data, or biometric data.
- Data concerning health.
- Data concerning an individual's sex life or sexual orientation.

Law enforcement purposes

"Law enforcement purposes" is defined as 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.

As a police force it is necessary to carry out sensitive processing to fulfil the functions of the Chief Constable as both a competent authority and responsible for the policing of Gloucestershire.

Section 35(4) and (5) of the Act states that sensitive processing for law enforcement purposes is permitted in only two cases:

a) the data subject has given consent to the processing for the specific purpose **and** at the time the processing is carried out, the controller has an appropriate policy document (APD) in place

or

b) the processing is strictly necessary for a law enforcement purpose, the processing

meets at least one condition in Schedule 8 of the Act **and** at the time the processing is carried out, the controller has an APD in place.

If either of these two conditions are met, the sensitive processing will be lawful.

The Data Protection Principles

The principles set out in Part 3 of the DPA require personal data to be:

1. Processed lawfully and fairly (lawfulness and fairness).

2. Collected for specified, explicit and legitimate law enforcement purposes, and not further processed in a way which is incompatible with those purposes (purpose limitation).

3. Adequate, relevant and not excessive in relation to the purposes for which it is processed (data minimisation).

4. Accurate and where necessary kept up to date (accuracy).

5. Kept for no longer than is necessary for the purposes for which it is processed (storage limitation).

6. Processed in a way that ensures appropriate security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (integrity and confidentiality).

In addition the controller is responsible for and must be able to demonstrate compliance with the above principles (accountability principle).

How we will meet these principles in relation to sensitive processing

Principle 1. Lawful and fair

GC will only undertake sensitive processing for law enforcement purposes where we have a lawful basis to do so and where the information is required for a specific reason.

We will communicate fair processing information to individuals through the GC website (Privacy Notice) and to individuals on request by contacting the Data Protection Team. The information can also be provided in different formats if needed.

Where consent is requested from an individual to allow sensitive processing, the individual will be provided with full details of what will happen to their data and the length of time it will be retained.

They will also be advised of the right to withdraw consent at any time before the information is processed. Where consent is requested, this information will be documented and available on request.

Where the processing involves the taking or retaining of relevant physical data where the consent of the individual is not required, the legislation includes but may not be limited to; Police and Criminal Evidence Act 1984, Criminal Procedure and Investigation Act 1996,

the Protection of Freedoms Act 2012, Crime and Security Act 2010 and Immigration and Asylum Act 1999.

The most common Schedule 8 condition which applies to law enforcement processing is:

- Condition 1 – Statutory purposes.

Other commonly used conditions are:

- Condition 3 – Protecting individual's vital interests; and
- Condition 4 – Safeguarding of children and of individuals at risk.

Principle 2. Specified, explicit and legitimate purposes

Sensitive processing will be restricted to only that which is necessary for the relevant law enforcement purpose and it will not be used for a matter which is not a law enforcement purpose unless that use is authorised by law. It may, however, be used for another law enforcement purpose by GC or another organisation that is authorised to carry out law enforcement processing.

Principle 3. Adequate, relevant and not excessive

Any personal data collected for law enforcement purposes will be restricted to that which is necessary for the purposes of processing. The mandatory data protection training for all officers and staff emphasises that police records must ensure that personal data is adequate, relevant, unambiguous and professionally worded. Matters of opinion, which are not fact, will be clearly recorded as such.

Principle 4. Accurate and where necessary kept up to date

We will ensure as far as possible that the data we hold is accurate and kept up to date. In some circumstances we may need to keep factually inaccurate information e.g. in a statement from a victim, witness or alleged perpetrator. All officers and staff are made aware of the need for accuracy and are responsible for the accuracy of the personal data they process. Checks are carried out on the accuracy of data during audits and line manager checks. Personal data found to be inaccurate will be rectified or erased whenever possible. Where this is not possible, there will be an addendum to that personal data advising of the inaccuracy. When necessary, the processing will be restricted in accordance with Sections 46 to 48 of the DPA. This will ensure that data will not be transmitted or made available for any of the law enforcement purposes.
If inaccurate personal data has been disclosed, the recipient will be advised of this as soon as practicable.

Principle 5. Kept for no longer than is necessary

GC has a Records Management, Retention and Disposal Schedule which outlines the principles which GC adhere to for the retention, review and disposal of records which have been created within its activities and functions. All sensitive processing will be dealt with under this Policy which is available on GC's website or can be sent direct by request to the Records Management Team.

When an individual withdraws consent to the sensitive processing (where consent has previously been provided by the individual), that data will be destroyed in line with legislative requirements.

When sensitive processing is carried out in accordance with a Schedule 8 condition, the information will be retained or destroyed in accordance with the Records Management, Retention and Disposal Schedule.

Principle 6. Appropriate security

GC has developed and implemented appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Technical measures - GC applies the information security standards set for the National Policing Community by the Cabinet Office and the Home Office. This includes encryption, firewalls, anti-virus software, IT health checks, vulnerability assessment and penetration process, user authentication, role based and password controlled access, technical assurance and technical audits and end point management.

Organisational measures - All officers and staff are required to undertake mandatory data protection training. All new staff, officers and contractors are vetted prior to being given access to GC information, systems and records.

Officers and staff receive training in how to use police systems before being granted access. Buildings are kept physically secure with access only being granted to individuals who require it for an authorised purpose.

Accountability principle

We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of a data protection officer who has a reporting line to our highest management level.
- Taking a ‘data protection by design and default’ approach to our activities.
- Maintaining documentation of our processing activities.
- Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors.
- Implementing appropriate security measures in relation to the personal data we process.
- Carrying out data protection impact assessments for high risk processing.

We regularly review our accountability measures and update or amend them when required.

Further measures include the following Policies:

- Data Protection Policy.
- Information Security Policy

Erasure of personal data

Erasure of personal data will be dealt with in accordance with Section 47 and (when necessary) Section 48 of the Act.

Retention and review of this policy

This policy document will be retained in accordance with Section 42 of the Act. It will be made available to the ICO on request.

The policy will be reviewed on an annual basis (or more regularly if circumstances require it) and updated as necessary at these reviews.