Data Protection Policy

Table of Contents

Section 1 – Policy Intentions 1
Section 2 – Policy wording 1
Section 3 - Related References: 9
Section 4 - Identification, Monitoring and Review 9

Section 1 – Policy Intentions

Gloucestershire Constabulary has a statutory obligation to process personal data in accordance with the provisions of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA). Where appropriate, these are referred to collectively as the data protection legislation.

This policy applies to individuals at all levels of the organisation including Police Officers, Police Staff, Special Constabulary, PCSOs, temporary staff and 3rd parties (for example but not necessarily limited to partner agency staff, consultants, contractors and volunteers) who have authorised access to personal data as part of their role. Everyone must have a clear understanding of their personal responsibilities under data protection legislation and how this affects the processing of personal data. This policy is intended to promote understanding and provide guidance in respect of the general requirements of the legislation.

Section 2 – Policy wording

What the Data Protection Act 2018 covers

The four main areas provided for in the Act are general data processing, law enforcement data processing, data processing for national security purposes including processing by the intelligence services and regulatory oversight and enforcement.

Processing by the Police splits into General Processing (covered by DPA Part 2) and Law Enforcement Processing (covered by DPA Part 3). General Processing includes all processing directly within the scope of the UK UK GDPR.

How is personal data defined?

The Act defines personal data as any information relating to an identified or identifiable living individual. An identifying characteristic could include a name, ID number or location data. You should treat such information as personal data even if it can only potentially be linked to a living individual.

General Processing (UK GDPR -Part 2 of the Act)

Part 2 of the Act relates to general processing and covers police support functions such as Human Resources, Occupational Health, Finance and Payroll (including pensions), Estates, ICT and Procurement. This means that UK GDPR applies in its entirety to these functions.

The UK GDPR does NOT apply to the processing of personal data by a competent authority (broadly speaking the Police and other Criminal Justice Agencies) "for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and the prevention of threats to public security".

Principles

The legislation sets out six principles which are the foundation of the requirements for good data handling. Personal data must be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes; (Purpose limitation)
3. Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed;(Data minimisation)
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; (Accuracy)
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals; (Storage limitation) and
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. (Security)

In addition organisations are responsible for and must be able to demonstrate compliance with the principles. This is known as the **Accountability principle** and applies to general and law enforcement processing. Steps taken by the Constabulary to comply with the accountability principle are as follows:

Adopting and implementing data protection policies;
Taking a 'data protection by design and default' approach;
Putting written contracts in place with organisations that process personal data on its behalf;
Maintaining documentation of processing activities;
Implementing appropriate security measures;
Recording and, where necessary, reporting personal data breaches;
Carrying out data protection impact assessments

Special Category Data

Special category data is personal data which the UK GDPR says is more sensitive, and so needs more protection. In order to lawfully process special category data, you must identify both a lawful basis under Article 6 and a separate condition for processing under Article 9. There are ten conditions for processing this data in the UK GDPR itself, but the Data Protection Act 2018 introduces additional conditions and safeguards. A condition for processing this data must be determined before you start processing and this must be documented.

Special category data could be; race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

The UK GDPR rules for special category data do not apply to information about criminal allegations, proceedings or convictions. There are separate safeguards for personal data relating to criminal convictions and offences, or related security measures and there must be a lawful basis for processing together with the need to comply with Article 10.

Article 10

"Processing of personal data relating to criminal convictions and offences or related 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 under the control of official authority"

Law Enforcement Processing (Part 3 of the Act)

Part 3 of the Act applies if you process personal data for 'law enforcement purposes' and covers processing "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".

Principles

The principles are broadly the same as those in the UK GDPR, and are compatible so will assist in managing processing across the two regimes. Transparency requirements are not as strict, due to the potential to prejudice an ongoing investigation. A Controller must be able to demonstrate overall compliance with all of the law enforcement principles which are:

1. Processing of personal data for any of the law enforcement purposes must be lawful and fair;
2. The law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and; Personal data collected must not be processed in a manner that is incompatible with the purpose for which it was originally collected;
3. Personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed;
4. Personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and; Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay;
5. Personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed. Appropriate time limits must be established for the periodic review of the need of the continued storage of personal data for any of the law enforcement purposes;

6. Personal data processed for any of the law enforcement purposes must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, “appropriate security” includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

Policing Purpose

Gloucestershire Constabulary will hold information relating to a range of individuals including victims, witnesses, complainants, suspects and offenders, in connection with the policing purpose as well as details of others who work for or with the Force.
All personal information is held and processed in accordance with the Data Protection Act 2018. Anyone working within Gloucestershire Constabulary may only use information in accordance with their policing duties.

Information held by Gloucestershire Constabulary may be shared with other organisations where this is necessary for a policing purpose, for example information is shared:-

- With Criminal Justice systems as part of the pre-charge and post-charge processes e.g. prosecuting someone through the Court.
- When working with partner agencies to reduce crime and disorder, and anti-social behaviour as required by the Crime and Disorder Act.
- With the Disclosure and Barring Service which provides information to organisations in order to enable them to make safer recruitment decisions by identifying potential candidates who may be unsuitable to work with children or other vulnerable members of society.
- With other Professional and Regulatory Bodies.

Information is shared where specifically required to do so by statute or by order of the court.
Gloucestershire Constabulary will also share information with partner agencies when the information is required to enable them to carry out their statutory responsibilities or where it is necessary to prevent harm to the individual or others.

Any disclosure of personal information should be carefully considered in accordance with legislation, policy and/or information sharing agreements. Please refer to the Information Sharing Policy for further information.

Consent Based Processing

If the processing of personal data relies on consent as the lawful basis, the consent must be clear, informed and freely given. The consent must also be granular so that separate and distinct options are provided depending on the purpose and processing. When asking for consent the following points should be noted:

- Consent must be freely given, specific, informed and unambiguous.
- Individuals must be advised why the data is needed and how the data will be used.
- Individuals must be advised that they can withdraw their consent at any time and be informed how they do that.
- A record of the consent should be maintained
- Consent should be reviewed and refreshed at regular intervals
- Consent must not be a precondition of a service.
- Individuals should positively opt in, there can be no default consent.

Registration / Notification

The Chief Constable is the Data Controller for Gloucestershire Constabulary and has delegated day-to-day data protection responsibility to the Data Protection Officer (DPO) who acts as the point of contact for the Information Commissioner's Office (ICO).

Use of Police Information and Offences

Any use of police information which does not fall within the above categories is deemed unlawful and may constitute a criminal offence under Section 170 of the Act. This states that a person must not knowingly or recklessly:

(a) obtain or disclose personal data without the consent of the Controller;

(b) procure the disclosure of personal data to another person without the consent of the Controller;

(c) after obtaining personal data, retain it without the consent of the person who was the Controller in relation to the personal data when it was obtained.

Gloucestershire Constabulary staff are aware that the Act creates personal liability and that obtaining, disclosing, retaining or procuring of police information for a non-work related purpose is strictly prohibited.

Information Rights
The Data Protection Legislation provides data subjects with a number of rights. If personal data is held by the Force for Law Enforcement purposes then the right to data portability and the right to object do not apply.*

All personnel should be aware of the rights which individuals have in respect of their information and the specific processes which exist in Force to enable them to exercise those rights.

The individual rights are:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure (right to be forgotten)
- Right to restrict processing
- Right to data portability*
- Right to object*
- Rights in relation to automated processing

Right to be Informed- Privacy Notice

Gloucestershire Constabulary have produced a privacy notice which explains why we collect and use personal data, whose personal data we handle, what types of personal data we handle, where we obtain personal data from, which lawful basis do we use to process personal data, how we handle personal data and how we keep it secure and who we disclose personal data to. The privacy notice also explains data subject rights including the right of access and provides advice on how to apply for their personal data which

may be held by Gloucestershire Constabulary. The privacy notice should be kept under regular review and if we plan to use personal information for a new purpose, we must update our privacy notice and communicate the changes prior to commencement of the new processing.

A copy of our privacy notice is available via our website and intranet and displayed in public areas, for example custody sites and enquiry offices.

The Constabulary have also produced and published Appropriate Policy Documents which explain how the Force complies with the principles of the legislation in the processing of special category and sensitive data.

It is a requirement to ensure signs are displayed where CCTV is in use.

Right of Access
The right of access is managed by the Information Disclosure team (ID) who process all Subject Access Requests (SARs) on behalf of Gloucestershire Constabulary in accordance with the Act. It is important for all staff to know how to spot a SAR as the request can now be made verbally. In the event that you or your department receive a Subject Access request, please forward the request as a matter of priority to ID. Further information is available on the Force website.

Right to Rectification

Individuals are entitled to have their personal data rectified if it is inaccurate or incomplete. It must be done within one calendar month but for general processing, this can be extended for a further two months in complex cases. Where no action is taken, individuals have the right to be informed of how to seek a judicial remedy.

Right to Erasure

Individuals have a right to have personal data erased in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected / processed;
- When the individual withdraws consent if consent is the lawful basis for the processing;
- When the individual objects to the processing and there is no overriding legitimate interest for continuing with the processing;
- When the personal data was unlawfully processed
- When the personal data has to be erased in order to comply with a legal obligation;
- When the personal data is processed in relation to the offer of information society services to a child.

Right to Restrict Processing

Where it is claimed that data is inaccurate or the right to erasure has been exercised, individuals can require the Controller to restrict processing until verification checks have been completed. Individuals may also require Controllers to restrict processing where there is no legal basis

Right to Data Portability – not applicable to Law Enforcement Processing

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

provided in a structured, commonly used and machine readable form. The information must be provided free of charge.

Right to object – not applicable to Law Enforcement Processing

Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling), and processing for purposes of scientific research and statistics.

Rights related to automated decision making including profiling
This gives individuals the right to object to decisions made about them on the basis of automated processing where those decisions have legal or other significant effects. This includes processing where there is no human intervention, for example where automated processes are used to sift recruitment applications.

Information Rights Process
The right to erasure and right to rectification are managed by the Records Management team in accordance with the Retention and Disposal Schedule.
Requests should be sent to: Records.Management@gloucestershire.pnn.police.uk

Data Subjects wishing to exercise any of the other rights should contact the ID team in the first instance- informationdisclosureunit@gloucestershire.pnn.police.uk

Exemptions

Crime and Taxation – The UK GDPR regulations relate to the processing of personal data for non-Law Enforcement purposes. The Data Protection Act 2018 sets out exemptions from the UK GDPR which apply in some circumstances. They mean that some of the data protection principles and subject rights within UK GDPR **DO NOT** apply at all or are restricted when personal data is used or disclosed for particular purposes.

The most relevant exemption for Law Enforcement is that within Schedule 2 Part 1 Paragraph 2 (Crime & Taxation: general). This applies where personal data is disclosed by an organisation subject to UK GDPR to the police for the purposes of the prevention or detection of crime or the apprehension or prosecution of offenders.

It restricts the application of UK GDPR data protection principles and subject rights to the extent that the application of those provisions would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

In effect the exemption means that an organisation can provide personal data to the police where necessary for the prevention or detection of crime or the apprehension or prosecution of offenders without fear of breaching UK GDPR or Data Protection Act 2018.

Vital Interests – UK GDPR Article 6(1)(d) provides a lawful basis for organisations to disclose personal data to the police where the disclosure is necessary in order to protect the vital interests of the data subject or of another natural person.

Data Protection by Design and Default- Data Protection Impact Assessments (DPIA)
A DPIA screening questionnaire and/or a full DPIA must be undertaken prior to the introduction of any new technology, new process or significant change in process involving personal data. The purpose of the DPIA is to identify and mitigate any privacy risks associated with the processing prior to commencement and throughout the lifecycle. Further information and templates can be found on the Force Intranet

Personal Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data'. Examples of a personal data breach are provided below:

- ➢ access by an unauthorised third party;
- ➢ sending personal data to an incorrect recipient;
- ➢ computing devices containing personal data being lost or stolen;
- ➢ alteration of personal data without permission;
- ➢ loss of availability of personal data or misuse of personal data
- ➢ cyber attacks

Any security breach that creates a likely risk to the rights and freedoms of the individual is notifiable to the ICO within 72 hours. Any personal data breach that is likely to result in a high risk to the rights and freedoms of an individual must also be notified to the individuals affected by the breach.

All staff must ensure that they are aware of the procedure to be followed in the event of a data breach and the location of the Security Incident Report Form on the Intranet.

Data Protection Officer

The appointment of a Data Protection Officer (DPO) is mandatory for a Police Force. The DPO is based within the Governance and Compliance Department and reports to the Head of Governance and Compliance and to the Information Governance Board chaired by the Deputy Chief Constable.

Data Processing

Where a Processor carries out processing on behalf of the Constabulary, a Data Processing Contract will be implemented to ensure that all Article 28 (UK GDPR)/ sections 59 and 60 (DPA) obligations are met. Any Data Processing Contract must be reviewed by the Data Protection Officer, Force ISO and /or the Force Solicitor prior to implementation except where a procurement service is used, in which case that service will provide appropriate specialist advice.

Information Security

UK GDPR, Article 5 (f), and the Data Protection Act Part 3 Section 40, require the Force to ensure that information is appropriately and adequately secured and that reasonable steps are taken to ensure the reliability of any employees who have access to personal data. Information Security refers to not only the physical or technical protective measures taken but also to issues such as the clear desk policy, use of e-mail and the Internet and the Government Security Classification (GSC). For further guidance, see the Information Security Policy and contact the Force Information Security Officer.

Training

Annual Data Protection refresher training is a mandatory requirement for all officers, staff, special constables, volunteers or other approved persons who have access to police information. The DPO will liaise with the Learning and Development Department to ensure this requirement is adhered to and line managers are responsible for ensuring that any non-completion of the training is followed up.

Section 3 - Related References:

This Policy must be read in conjunction with the following supporting documentation:
Information Security Policy
Records Management Policy
Retention and Disposal Schedule
Appropriate Policy Document (SCPD)
Appropriate Policy Document (Sensitive Processing)
Acceptable Use Policy
Internet Security Policy
Email Security Policy
Government Security Classification Policy
Vetting Policy
Information Sharing Policy
NPCC Data Protection Manual of Guidance
College of Policing APP Data Protection
ICO Guidance
Security Incident Report Form
Security Incident Process
Information risk management policy

Section 4 - Identification, Monitoring and Review

The Policy should enable consistent and effective decision making. Where operational or managerial circumstances require any decision making that would adversely affect adherence to the policy or procedure, in line with the 'Statement of Intent' of the constabulary and the police service 'Code of Ethics', if an officer/ police staff member believes that they need to make a decision that steps outside of policy and procedure they should do so, provided that:

- the officer/ police staff member raises the matter at the earliest opportunity (and ideally before any such decision is made) with their line manager declaring their intended (or actual) course of action if notification is made after the decision is taken,
- produces, in a timely manner, a signed and dated written explanation of why it is/ was deemed necessary to step outside of policy and procedure, and
- maintain an adequate record of this written rationale for audit purposes appropriate to the circumstances/ contravention

GSC Security Marking:	**Not Protectively Marked**
Type:	**Policy**

Department	**URN**	**Strategic Board 'signed off'**	**Author/Reviewer**
Governance and Compliance	**023**	**IGB**	**Force Data Protection Officer**

Version	**Date**	**History of changes (ensure public copy amended and uploaded to external website)**	**Complied with Policy Guidance**
Version 4	**May 2019**	**Policy reviewed for the DP Act 2018 /UK GDPR**	✓
Version 4.1	**November 2020**	**Section 1- Insertion of UK GDPR, Section 2- addition of wording around accountability principle, consent**	

		processing, annual DP training and Appropriate Policy Documents. Change of process for right to erasure and right to rectification requests. Minor revisions to reflect the fact that legislation is no longer new.	
Version 4.2	**November 2022**	**Deletion of Brexit wording relating to the change to UK GDPR. Minor revisions to reflect process/policy intention/ information sharing policy. Reference added to retention and disposal schedule,GSC Policy and Information Sharing Policy.**	

Formatting and Publication:	**Governance and Compliance Team**
Next Document Review Date:	**September 2023**

EIA	**EIA Sign Off – name and date**	**EIA Review – name and date**
LOW		

Link to EIA – *G&C to complete hyperlink action*

FREEDOM OF INFORMATION - This version will be placed on the public domain website

If this version <u>CANNOT</u> be placed on the public domain website, please provide a FOI redacted version.	**Permission given to place on external website**

Previous policies can be found with the Governance and Compliance team.