Data Protection

Policy & Procedure

Greater Manchester Police

October 2016

Table of Contents

1. Policy Statement

GMP must, when processing personal data, discharge its obligations under the Data Protection Act 1998 (DPA), which regulates the way in which organisations handle personal data. To reduce risk to the Force and to those individuals whose data is held, it is vitally important that all staff and officers are aware of their responsibilities under the Act.

The DPA mandates the dissemination of legal requirements, policy and procedures to all staff. In implementing these obligations GMP follows the guidelines for infrastructure and lines of accountability set out in ACPO's Data Protection Manual of Guidance.

The policy supports GMP's business purposes to protect public safety, and prevent crime and disorder, by promoting a culture of safeguarding the personal information held by GMP and assuring its quality.

1.1 Aims

To explain GMP's responsibilities under the Data Protection Act 1998 (DPA) and related legislation, in respect of personal information, and to provide guidance about using information securely and lawfully, in line with force strategy on information governance and information assurance.

Specifically this policy aims to:

- Inform all officers and staff of their roles and responsibilities in relation to the DPA;
- Ensure that GMP's processing of personal information is compliant with the DPA;
- Protect the rights and freedoms of individuals under the DPA and associated legislation;
- Maintain the integrity and quality of information used for policing purposes;
- Ensure that officers and staff are aware of the consequences of non-compliance.
- Ensure that disclosures to third parties are managed in compliance with legislation

2. Scope

This policy applies to all personal information (as defined by the Act – see Section 4) recorded and processed by all members of GMP. This means any recorded verbal, written, electronic, photographic and paper based information, from which living individuals can be identified.

3. Roles & Responsibilities

The Chief Constable is the notified **Data Controller**

Assistant Chief Officer (Business Resources) – **Senior Information Risk Owner** - takes responsibility for managing risk associated with information compliance matters.

Information Compliance and Records Management Unit Manager **- Force Data Protection Officer,** the lead on data protection policy and procedure

Information Compliance and Records Management Unit (ICRMU): Data Protection Subject Matter Experts for the Force. A list of contacts is available on the intranet. The Unit:

- Handle requests for information under DPA (s.7– subject access), Freedom of Information Act (FoI) and Environmental Information Regulations (EIR). They are also responsible for disclosures in relation to insurance under the ACPO/ABI agreement, disclosures under the Notifiable Occupations Scheme and the Criminal Injuries Compensation Authority (CICA).

- Advise on statutory compliance for all business processes, deal with disclosures to other organisations, handle complaints, develop information-sharing and data processing agreements, undertake audits of force systems, and promote good practice.

Information Security: Assure security of IT systems

Professional Standards Branch: Will investigate potential misconduct in relation to breaches of data protection and information security

All officers/staff: Should be aware of their responsibilities under the Data Protection Act and in relation to the handling and processing of personal data.

4. Terms and Definitions

The Data Protection Act

The DPA regulates the processing of personal data by organisations, whether it is held on paper or in electronic form. The DPA is designed to protect people's personal data against unlawful use, by imposing data protection principles upon organisations, and providing individuals with rights.

Processing that breaches the principles, or is contrary to individual rights, is unlawful. All personal data processed by GMP is covered by the DPA. Personal data held by GMP must only be used in connection with legitimate purposes and must be protected from any unauthorised or unlawful processing.

If an individual knowingly or recklessly breaches any part of the DPA, such as improperly accessing or disclosing personal data, then s/he may be guilty of a criminal offence.

Personal Data

Personal data is data relating to a **living** individual who can be identified from that data, or from that data together with other information held by GMP. Personal data can consist of information recorded in paper or electronic form (including that held on storage devices) and can include text, biometrics, and images (including photographs, CCTV, vehicle cameras and body camera footage). The Chief Constable is the Data Controller for this data.

Sensitive Personal Data: some categories of data are deemed Sensitive. Under the DPA, Sensitive Personal Data is data with the following characteristics:

- racial or ethnic origin of the data subject
- political opinions
- religious beliefs
- trade union membership
- physical or mental health condition
- sexual life
- commission or alleged commission of any offence
- any proceedings for any offence or alleged offence

Much of the personal data held by GMP will fall into this category, and it requires additional safeguards for processing. Schedules 2 and 3 of the DPA specify exactly what conditions must be met for processing "Personal" and "Sensitive Personal" data. (See Appendix and source documents)

Processing includes **any** use of personal information, such as:
collecting, holding, using, updating, viewing, accessing, disclosing, archiving and disposal.

The **Data Protection Principles**

1. Personal data should be processed fairly and lawfully.
2. It should be obtained only for specified and lawful purposes, and not processed further in a manner incompatible with those purposes.
3. It should be adequate, relevant and not excessive.
4. It should be kept accurate and up to date.
5. It should not be kept longer than necessary
6. It should be processed in accordance with the rights of the data subject
7. Appropriate technical and organisational measures should be taken against unauthorised or unlawful processing, loss, destruction or damage.
8. It should not be transferred outside the European Economic Area without an adequate level of protection (See Appendix for list of countries).

Other important definitions under the DPA can be found in the Appendix.

5. Procedure

5.1 Use of personal data

You are responsible for ensuring that personal data in your care is processed properly, not only to comply with the legislation but also to maintain the integrity of the information and the confidence of the public that their personal data is in safe hands.

GMP has notified the Information Commissioner's Office (ICO), the data protection regulator, of the purposes for which personal data will be processed see Appendix for further details). You should only use personal information for a legitimate policing purpose, or in support of such a purpose.

The policing purposes are: Prevention and detection of crime, apprehension and prosecution of offenders, maintenance of law and order, protection of life and property, vetting and licensing, public safety, rendering assistance to members of the public in accordance with force policy.

Other legitimate purposes are those related to staff administration.

5.2 Collection and recording

- Exercise care when collecting, processing or disclosing any personal data on behalf of GMP and do so only when it is necessary for your duties and it supports a policing purpose.
- Ensure the information you record is accurate, adequate for the purpose, not excessive, and worded clearly and unambiguously. Check existing records to make sure you are not creating duplicates.
- Do not record irrelevant or inappropriate remarks about individuals because anyone has a right to see personal information that we hold; this could lead to claims for compensation and/or enforcement action against the force (see below). Be aware that any data, personal or not, that you create and record, is potentially disclosable under the DPA, FoI or EIR.
- Consult the Information Governance Unit about any new or revised processing.
- Abide by force retention guidelines (see Retention Schedules), do not keep information longer than is necessary and do not keep copies of information "just in case" beyond their retention periods.

5.3 Disclosure

- Use personal data only in line with the purpose for which it was collected.
- Do not disclose it to any other person unless you are authorised to do so by GMP. If in doubt ask your line manager, or the IGU.
- The information you disclose should be adequate, relevant, and not excessive for the purpose for which the disclosure is made.
- Be aware that if you make or encourage another person to make an unauthorised disclosure knowingly or recklessly you may be held criminally liable.

5.4 Information security

- Apply the Government Protective Marking Scheme (GPMS) to all documents and communications
- Keep your passwords safe. Do not disclose them to anyone. You should change your passwords regularly.
- Follow clear desk policies, and practise screen-locking.
- Manage your e-mails in such a way that they can be easily identified, stored and deleted
- Only access a Restricted or Confidential computer system when you have a policing purpose to do so, and complete the audit trail information on each occasion
- Ensure papers or any other media containing personal data are not removed from GMP premises without suitable security measures (in line with current orders) and are not left in insecure areas;
- Avoid accidental disclosure by fax, voice or text by ensuring that you know and follow guidelines for sending faxes and call-back procedures. Be aware of auto-populating addressee lines in email, to avoid information being sent to the wrong recipients.
- Work to a high level of accuracy. When sending e-mails and faxes, make sure both the message content and destination are accurate, and in compliance with GPMS
- When no longer required, dispose of personal information as confidential waste
- Do not upload information to social networking sites without authority.

5.5 Training

Undertake data protection training as directed by your line manager; in particular the following NCalt e learning training packages should be completed by all staff handling personal information:

- Data Protection Foundation Level Ncalt package
- MOPI 1 – Background to MOPI Ncalt package

The Data Protection Foundation Level (or most current equivalent Ncalt package) should be repeated every three years to refresh and update your knowledge.

5.6 Liability for breaches

It is not just the data controller who is criminally liable. All GMP staff are considered servants or agents of the Chief Constable (the data controller) and can be personally criminally liable if they disclose or obtain personal data without the authority of the data controller. Therefore if you make, or encourage another person to make an unauthorised disclosure knowingly or recklessly, you may be held criminally liable. Section 55 DPA offences are to:

- Knowingly or recklessly unlawfully obtain or disclose personal data;
- Knowingly or recklessly sell or offer for sale the personal data.

In addition, the following actions are criminal offences under the Computer Misuse Act 1990:

- Unauthorised access to computer material (‘hacking’);

- Unauthorised modification of computer material; and
- Unauthorised access with intent to commit or facilitate the commission of further offences.

5.7 Operational application of the Data Protection Act

5.7.1 Working with the Information Compliance and Records Management Unit (ICRMU)

- If you receive a request for personal information that you think may be a subject access request under the DPA, or a request under the Freedom of Information Act (FOI), or the Environmental Information Regulations (EIR), forward it to the ICRMU
- If you create a GMP Twitter account or other social networking account, you should ensure it is checked regularly for such requests.
- If you are asked to supply information by the ICRMU Assistant for subject access or FOI purposes, do so promptly so that statutory deadlines can be met
- The ICRMU will provide training and advice to front-desk staff who handle subject access applications
- If you are asked for information by the ICRMU Officers, you should respond to them promptly. This may be in relation to complaints about processing of personal data, assessment of force compliance, or #TE monitoring.
- If you receive a complaint from a member of the public relating to a disclosure, or the accuracy of their personal data, please refer it to the ICRMU.

5.7.2 Compliance Assessments

Before amending an existing process or introducing a new process involving personal data, you should consult the ICRMU so that an assessment can be conducted. A ‘process’ is any operation covered by the definition of ‘processing’ as defined above, and is not restricted to the development or enhancement of IT systems. This will ensure that the activity is compliant with the Data Protection Principles, and reduce risk to the Force.

5.7.3 Privacy Impact Assessments (PIA)

A PIA helps assess the impact of a data processing activity (such as collection or disclosure of information) on the privacy of individuals, and assists in considering the implications for the Force. PIAs help identify privacy risks, foresee problems and bring forward solutions.

A PIA is recommended where sensitive personal information is to be shared or collected in a new way. It is also recommended where new and intrusive technology is being used or where personal information, originally collected for a different purpose, is going to be reused in a new and previously unexpected way. Effective assessment can prevent damage to the Force’s reputation and the public purse, by reducing opportunity for costly privacy breaches such as data loss.

The project manager, with the assistance of the ICRMU, is responsible for conducting the assessment.

5.7.4 Subject access (s.7 DPA)

A person is entitled:

- To be told by any organisation whether any information is being processed about him or her;
- If so, to be given a description of the personal data, the purposes for which the data is being processed, the source of the data, and those to whom it may be disclosed. Exemptions may apply.

This is known as a Subject Access Request. The response to an application must be sent within 40 calendar days of receipt. This process is handled by the Information Compliance and Records Management Unit.

Police officers have an additional right of Access to Personal Files (via Police Regulations).

Important:

- The right to access personal information under the DPA is different from rights under the Freedom of Information Act (FOIA).
- The FOIA provides the right to information held by a public body (except for personal information).

There are other individual rights under the DPA – see the Appendix at Section 8.

5.7.5 "Fair processing"

To comply with the first data protection principle (Personal data should be processed fairly and lawfully) a data controller should tell individuals, when collecting their personal data, about what they intend to do with it. Clearly it is not practical to do this for the majority of personal data collected in the course of operational policing, and it would not be a reasonable expectation, but it should be a consideration for routine administrative processes, e.g., neighbourhood contacts, or job applications, and for partnership initiatives. For further advice, contact the ICRMU.

A statement about what GMP does with personal data (known as a Fair Processing Notice or a Privacy Notice) can be found on the GMP website.

5.7.6 Exemptions and Disclosures

A general rule of data protection is an assumption of non-disclosure of personal information. A number of exemptions under the DPA can be applied to policing operations.

- Section 29 (3) DPA (using Personal Data Disclosure form 819B) - provides an exemption from non-disclosure when the disclosure is for a policing purpose, (i.e, for the prevention or detection of crime, or the apprehension or prosecution of offenders). The police can ask another organisation for information, and s.29(3) will allow that organisation, if they believe it is justified, to release information to the police. You should note that s.29(3) is not an instruction for them to supply the police with the information; it is a power of release, not a power to request.

- Section 35 DPA provides exemptions from non-disclosure, for compliance with legal obligations or for the purposes of legal proceedings or prospective legal proceedings.

Other exemptions in the DPA may be applied to Subject Access applications, for example when disclosure would compromise policing operations or the privacy of third parties.

Further exemptions may be relevant to particular parts of the organisation, such as the Corporate Communications Branch, where s.32 may provide an exemption for journalistic purposes, or the External Relations and Performance Branch, where s.33 relates to research.

Besides the DPA there is additional legislation that may require or permit disclosure in certain circumstances. For example, under the Police Act 1997 the police have a duty to disclose relevant personal data for CRB Disclosures. The Crime and Disorder Act 1998 provides a power for certain public authorities to share information for the purpose of preventing crime and disorder.

5.7.7 Information Sharing

Information Sharing Agreements, Data-processing Agreements, Research Agreements

If you are involved in partnership working where personal data is exchanged on a regular basis (information sharing), or using the services of a third party who will be processing data on behalf of GMP (data processing), you must ensure that the correct protocols and sharing agreements are in place, stating legal gateways that underpin disclosures, what information is to be shared, and how the data is to be used and how it is to be handled and protected.

The purpose of an agreement is to ensure force data is afforded the necessary safeguards, and to set out in advance the conditions of use of the data, and to agree processes and procedures, so that requests for disclosure, between organisations, do not have to be assessed on every occasion. Proposals for new multi-agency initiatives or changes to existing agreements should be sent to the ICRMU for consultation and approval.

Research agreements (where a student or academic institution requests access to GMP data) should be referred in the first instance to: Strategy, Planning and Policy Section, External Relations & Performance Branch.

You should refer to the Information Sharing Policy for further information. In addition, the ICRMU has produced guidance notes and a repository of all current agreements, which can be found on SharePoint within the Document Centre.

5.7.8 Audit and monitoring

The ICRMU examines, by way of audit, the processing of all force information.

The overriding purpose of an audit is to ensure that personal data processed by GMP is obtained, held, used and disclosed in accordance with the DPA.

The principal objectives of auditing force information are to:

- Assess compliance with the DPA;
- Assess compliance with the force policies in relation to data protection;

- Identify potential gaps and weaknesses in processing;
- Quantify risk to the organisation, and make recommendations to minimise that risk;
- Measure accurately and consistently the occurrence of non-compliance and operationally critical errors;
- Allow comparison of non-compliance and error rates with OPCC, HMIC and ACPO
- Increase the level of data protection awareness among management and staff.

One element of this activity is monitoring of transactions on both the PNC (#TE checks) and PND; this is a national requirement. You may be asked to provide information to support any enquiry you have made.

6. Associated Documents

Legislation

- Data Protection Act 1998 (DPA), including statutory conditions for processing of personal data Schedules 2 and 3
- Statutory Instrument 417/2000 (Processing of Sensitive Personal Data Order)
- Computer Misuse Act 1990
- Human Rights Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Privacy and Electronic Communications Regulations 2003

National Policy

- ACPO Data Protection Manual of Guidance
- APP Information Management
- ICO Subject Access Code of Practice
- ICO Employment Practices Code of Practice
- ICO CCTV Code of Practice
- ICO Information Sharing Code of Practice

GMP Policy

- Information Sharing Policy
- Records Management Policy (draft)
- Government Protective Marking Scheme Procedure
- Appropriate Use of Electronic Communications and Information Systems Policy
- Use of DPA Section 29(3) (2014/23)
- Statement on how GMP uses personal data (“Fair processing notice”) (This will appear on the website)
- Access to GMP Intelligence Systems (CCO 2007/35)
- Access to force computer systems and information (CCO 2003/24)

7. Statutory Compliance

7.1 Data Protection Act (1998)

This Policy and Procedure has been drafted by the Information Compliance & Records Management Unit and complies with the Data Protection Act 1998

7.2 Freedom of Information Act (2000)

This policy is disclosable under the FOIA. Up to and including section 4 can be immediately published. Section 5 - Procedure and onwards, would be considered for disclosure on request and assessed by the Information Complianceand Records Management Unit.

7.3 Equality Act 2010

The Policy and Procedure will not have any effect on equality for any of the protected characteristics. It relates to compliance with the Data Protection Act and the provision of indivual rights afforded by that Act and by the Human Rights Act. Sensitive personal data as defined by the Act includes race, religion or belief, sexual life and additional obligations are placed on the data controller by the Act when processing data of this nature.

8. Appendices

8.1 DATA PROTECTION ACT 1998: Further Information

Definitions

“Personal data” is data relating to a living individual who can be identified from that data, or from that data together with other information held by GMP.
“Sensitive personal data”: some categories of data are deemed sensitive under the DPA – these include a person’s racial/ethnic origin, political opinions, religious belief, trade union membership, physical/mental health, sexual life, commission of offences, or court proceedings in respect of offences.

Processing includes any use of personal information, such as: collecting, holding, using, updating, viewing, accessing, disclosing, archiving and disposal.

The DPA is regulated by the Information Commissioner’s Office (ICO).

Notification: We are required to register details of our processing with the ICO: GMP Register entry. This includes the type of data we process and sets out our purposes for doing so, which are:

The policing purposes: Prevention and detection of crime, apprehension and prosecution of offenders, maintenance of law and order, protection of life and property, vetting and licensing, public safety, rendering assistance to members of the public in accordance with force policy.

In addition we register processing for staffing and administrative purposes.

The Data Controller determines the purposes for processing the information, and the way it is done. The Chief Constable is the data controller for all GMP data, but the discharge of his duty is delegated as shown under Roles and Responsibilities.

People whose data is processed are known as data subjects. These may be offenders, victims, witnesses, officers, staff, etc.

The Principles - 8th Principle: Personal data should not be transferred outside the European Economic Area (EEA) without an adequate level of protection.
The EEA countries are:
Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, the Republic of Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.

Conditions for processing personal data

Before any processing can take place legitimately, at least one condition listed in DPA Schedule 2 must be satisfied. The conditions are more stringent when dealing with Sensitive Personal data, when a condition listed in Schedule 3 must also be satisfied.

Conditions include, for example: consent of the data subject, necessary for the administration of justice, necessary in the vital interest of the data subject.
For further information see:

- Personal data - Schedule 2 of the DPA
- Sensitive personal data – Schedule 3 of the DPA and SI 417/2000

Schedules 2 and 3

Individual rights

The DPA provides individuals with the following rights:

Section 7: Subject access rights
Section 10: Right to prevent processing likely to cause damage or distress
Section 11: Right to prevent processing for the purpose of direct marketing
Section 12: Rights in relation to automated decision-taking
Section 13: Compensation for failure to comply with certain requirements
Section 14: Rights in relation to rectification, blocking, erasure and destruction
Section 42: Right to ask the Information Commissioner for an assessment as to whether an organisation is in breach of the data protection principles in respect of their personal information

Criminal offences

The data controller is guilty of an offence if he or she:

- Fails to fulfil the Notification requirements
- Fails to comply an Information Notice or Enforcement Notice;
- Knowingly or recklessly makes a false statement in compliance with an information notice or special information notice;

- Intentionally obstructs, or fails to give reasonable assistance in the execution of a warrant.

An individual may be charged with the following offences under s.55:

- knowingly or recklessly unlawfully obtain or disclose personal data;
- knowingly or recklessly sell or offer for sale the personal data.

Consequences of non-compliance

- The ICO regulates compliance with the DPA. Failure to comply with the DPA principles exposes the force to the risk of enforcement of legal action from the ICO or data subjects, and adverse publicity.

- When a potential breach of data protection is brought to the ICO's attention (often by way of complaint from a member of the public), the ICO will contact the ICRMU in the first instance. This may be about unlawful processing, disclosure or loss of personal data, or non-compliance with subject access provisions.

- If a breach is determined the ICO may require an organisation to take certain steps to achieve compliance, or may issue an Information Notice, requiring an organisation to issue specified information. Failure to comply may constitute a further breach and an Enforcement Notice may be served. The ICO can now issue penalties of up to £500,000, and data protection breaches can result in prosecution or imprisonment. The ICO has powers to enter an organisation's premises, view records, interview staff and observe record processing to establish if the organisation is in breach of the Data Protection Principles. The ICO can also, in certain circumstances, conduct their own audits on organisations' premises.