GREATER MANCHESTER POLICE

**Date:** 29/10/2024
**Our ref:** 01/FOI/24/013395/R

**FREEDOM OF INFORMATION REQUEST REFERENCE NO: 01/FOI/24/013395/R**

I write in connection with your request for information dated 04/10/2024, received by Greater Manchester Police (GMP) for the following information:

1. ***Please can you provide me with a copy of your current Information Classification Policy or Procedure or equivalent, including any related documents that address how information generated by the Force should be marked, stored, transmitted, destroyed etc. depending on their marking.***

***For example, markings that may be used - public, internal, sensitive, official, secret etc.***

2. ***I would also like to request your current risk review matrix or equivalent - likely to be in the form of a table/ process and explanation that allows for information management risks to be adequately reviewed (e.g. as you would use to assess a systems outage, data breach event, or loss of service etc.). This is probably based on a review of impact vs likelihood, to give a numerical score which provides a risk output (low, medium, high, critical for example).***

**Result of Searches**
Following receipt of your request searches were conducted within Greater Manchester Police (GMP) to locate the requested information and I can confirm that some of the information requested is held by GMP.

However, I am not obliged to supply you with all the information as an exemption applies.

Section 17 of the Freedom of Information Act 2000 requires Greater Manchester Police, when refusing to provide such information (because this information is exempt) to provide you, the applicant, with a notice which: (a) states that fact, (b) specifies the exemption in question and (c) states (if that would not otherwise be apparent) why the exemption applies.

Where redactions in the attached documents for question 1 have been made, that information is exempt from disclosure by virtue of the following exemptions:

**Section 40(2)(a) – Personal Information**
**Section 31(1)(a)(b) – Law Enforcement**

Where Section 40 has been used, this represents information that identifies a living individual, to disclose this information would breach the principles of the GDPR and the Data Protection Act 2018. Personal data is defined by Article 4 of the GDPR and Part 1 of the Data Protection Act 2018, and means any information relating to an identified or identifiable natural person ('data subject'). An identified natural person is one who can be identified directly or indirectly from that data.

Section 31 is a qualified and prejudice-based exemption and as such, subject to a harm and public interest test

**Harm**

To provide the redacted information within the attached policy would reveal policing tactics used by Greater Manchester Police. This would give an advantage to that are intent on committing offences and avoid detection. It would also increase the risk of danger towards the public GMP who sworn to protect. Some data has been redacted as those with questionable intentions could utilise this information for their gain to corrupt, obtain and / or generally misuse information.

**Public Interest Test**

**Factors Favouring Disclosure**

To disclose the redacted information would provide the public with a slightly more in-depth knowledge into how Greater Manchester Police operates. This would enable the populous to take steps to protect themselves against criminal activity and may lead to further information being provided to the force.

**Factors Favouring Non-Disclosure**

Conversely to the factors in favour of disclosure, to release the redacted information into the public domain would reveal the policing tactics of Greater Manchester Police. This would impact on the force's ability to detect and prevent crime and apprehend and prosecute offenders.

The risk of danger to the public would be increased by revealing such policing tactics into the public domain. The safety of the public we protect is of paramount importance to Greater Manchester Police and we would not wish to jeopardise that safety by releasing exempt information into the public domain.

**Balancing Test**

The arguments for and against disclosure of information need to weigh against each other. In this case the greatest argument for disclosure is the fact that the populous would be provided with information regarding how the force police operate.

However, given that the disclosure would increase the risk of increased crime to and assist those intent on committing crime to avoid detection the balance of disclosure, at this time, weighs on non-disclosure for those particular redacted parts of the policy requested.

This letter acts as a refusal notice for the redacted parts of the attached documents.

**Question 1.**

Please see the attached (redacted) documents.

**Question 2.**

No information held.

# Government Security Classifications (GSC)

## Policy & Procedure

**Greater Manchester Police**

**April 2023**

**POLICY & PROCEDURE IMPLEMENTED:** April 2023

**REVIEW DATE:** April 2025

**POLICY & PROCEDURE OWNER:** [redacted]

**APPROVED BY:** [redacted]

**IS THE POLICY & PROCEDURE NEW OR REVISED?** Revised

| VERSION NO. | DATE | SUMMARY OF CHANGES | AUTHOR(S) | [redacted] |
|---|---|---|---|---|
| 1.0 | Mar 2019 | New procedure – replacing the Government Protective Marking Scheme Procedure. | [redacted] | |
| 2.0 | Jan 2023 | Additional information and conversion from Procedure to Policy and Procedure template. | [redacted] | |
| | | | | |
| | | | | |

## Table of Contents

# 1. Policy Statement

This policy and procedure document describes how Greater Manchester Police (GMP) classifies information to ensure it is appropriately protected; how it supports the business and the effective exploitation of information; and how it meets the requirements of relevant legislation such as the Data Protection Act 2018 (DPA), Freedom of Information Act 2000 (FOI) and the Official Secrets Act 1989 (OSA).

The National Police Chiefs' Council (NPCC) agreed that all forces should adopt the Government Security Classifications (GSC) in 2016, which replaced the earlier Government Protective Marking Scheme (GPMS).

All employees have a duty to respect the confidentiality of any GMP information that they access and are personally responsible for safeguarding it in line with this document.

## 1.1 Aims

The aim of this policy and procedure is to provide guidance on how to handle information using the GSC.

As most of the information processed in GMP will be categorised as OFFICIAL, the purpose of this document is to:

- Safeguard the organisation's information
- Protect the personal data (PD) relating to data subjects
- Protect the organisation from potential legal liabilities, reputation and scrutiny from the Information Commissioners Office
- Ensure that all individuals understand the classifications and aid in their application
- Establish the minimum security standards necessary when working with police information
- Act as a supporting document to the national mandatory e-learning module "Introduction to Government Security Classifications (GSC)" on [redacted]

# 2. Scope

All GMP employees and others who have access to information for any purpose are required to comply with this policy and procedure. It is important that they know how to adequately protect information and understand how to classify it according to the sensitivity of its content.

The below individuals are therefore required to comply with this procedure:

- Police officers (all ranks)
- Police staff (all grades)
- Special officers (all ranks)
- Partners
- Agency workers
- Volunteers
- Contractors
- Visitors

- Staff working with the Office of the Deputy Mayor
- Staff working with the Greater Manchester Shared Services

This policy and procedure is applicable to information assets (IA) such as documents, records, files, data, and information that is captured, stored, processed, generated, or shared to deliver services and conduct business. For the purpose of this document the information assets will be termed 'information'.

## 3. Roles & Responsibilities

The GSC system places an emphasis on personal responsibility and accountability of individuals in exercising good judgement.

All information must be subject to appropriate protection and is subject to the 'need to know' basis. It is the responsibility of Information Asset Owners (IAOs) to ensure that this is enforced in respect of information (including personal data) for which they are responsible.

It is the responsibility of all individuals to assess the level of classification that should be applied to information to ensure it receives the appropriate protection.

Individuals must decide if there is anything sensitive about the information and classify it accordingly. They must also decide if adding a handling rule is necessary, to ensure that the data is adequately protected, and only disseminated to a controlled audience.

Information should only be shared with those who have a legitimate need to see it.

## 4. Terms and Definitions

| Abbreviation/Acronym/Term | Full Name/Descriptor/Definition |
|---|---|
| CESG | Communications Electronics Security Group |
| CINRAS | Communications and Cryptographic Incident Notification, Reporting and Alerting Scheme (managed by CESG) |
| CPNI | Centre for Protection of National Infrastructure |
| Data Subject | A data subject is a living individual who can be identified by the data that relates to them. |
| DPA | Data Protection Act 2018 |
| DV | Developed Vetting |
| FOI/FOIA | Freedom of Information |
| GMSS | Greater Manchester Shared Services |
| GSC | Government Security Classification (replaced the GPMS) |

| | |
|---|---|
| Handling Rules | Handling rules should define how the individual wishes the information to be protected, including limits on its distribution, transmission and/or storage.<br><br>Handling rules can be used to support the 'need to know' basis and RBAC by indicating the nature of the information, how it is handled, and ensuring that it is only available to those authorised to have access. |
| IA | Information Asset<br>An IA is a single data item or body of data defined and managed as a 'single unit' so that it can be understood, shared, protected and exploited effectively. Information assets have a recognised and manageable value, risk, content, and lifecycle. Information Assets can be made up of documents, records, files, data and information and information systems. Examples of an IA are; briefing documents, emails, documents relating to the investigation of a crime or incident, documents relating to personnel including HR files and development plans. This is not an exhaustive list. |
| IAA | Information Asset Administrator |
| IAO | Information Asset Owner<br>IAOs must be senior/responsible individuals involved with running the relevant business areas. Their role is to identify what information, especially personal data, is being stored, collected, what the retention and disposal requirements are, who can access the information and if any sharing of the personal data occurs and why. These individuals need to have a good understanding of the business needs for the information and address any risks associated and ensure that any PD is used fully within the law. |
| ICT | Information and Communications Technology |
| ISO | International Organisation for Standardisation |
| MV | Management Vetting |
| Need to know basis | This is an old term that implies, that colleagues must only have access to the information that they need to have access to, in order that they can carry out their roles. As more information is now held electronically, the more modern term is known as Role Based Access Control (RBAC). |
| NPCC | National Police Chiefs Council |
| NPPV | Non-Policing Personnel Vetting |

| | |
|---|---|
| Personal Data | Any data relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person |
| Role Based Access Control | RBAC is an access control method that assigns IT Systems permissions to end-users based on their role within GMP. |
| Sensitive and Special Category data | Sensitive or Special Category Data is PD which reveals or concerns racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. If the previous can be inferred from any information relating to a data subject, then it is classed as SD/SCD. |

# 5. Procedure

## 5.1 GSC Overview

GSC is a security control to assist with protecting Force information; it is a core requirement to support effective policing and its use is mandatory.

All Force information has value and requires a basic level of protection. The Force holds a very wide range of information and delivers many different services, but many of the information risks the organisation must manage are broadly similar.

GSC does not need to be applied retrospectively to existing information but applies to any new information within the organisation. Any previous classification should be updated when documentation or assets are subject to review.

Information must be classified in line with the GSC scheme. The marking applied to the information must be based on the possible impacts that could arise from any form of compromise, for example:

- Breach of confidentiality through the information being disclosed or revealed to those without a 'need to know' basis
- Information being exposed to alteration or unauthorised changes, such that it may not be able to be relied upon
- Information not being available to those who need it, when they need it

Applying a classification to information indicates to others the appropriate level of handling and controls required to protect it against such compromise.

All classifications and associated protective measures should be based on the information contained within this document and enforce the principle of 'need to know'.

### 5.2 GSC Primary Classifications

Security classifications indicate the sensitivity of information in terms of the likely impact resulting from the compromise, loss or misuse of the data and the need to defend against a broad range of threats.

Under GSC, one of the primary classifications may be applied:

- OFFICIAL
  - OFFICIAL-SENSITIVE plus handling rules to be used with a Descriptor (see 5.3 and 5.4)
- SECRET
- TOP-SECRET

Classifications, when required, should appear in full at the very top and bottom of each page of the documents, records, files, data, and information.

Unmarked information can still be sensitive and require appropriate protection. Equally, the presence of a classification does not mean that the material should not be disclosed in appropriate circumstances. Any disclosure must be in accordance with current Force policies, procedures, and statutory obligations.

If you are copying information from another source, you must consider the previous classification when applying a classification to your document/email. The classification you apply cannot be lower than the classification on the original piece of information.

#### 5.2.1 OFFICIAL Classification

All information captured, stored, processed, generated, or shared by the Force has a minimum classification of OFFICIAL by default. It includes routine business operations and services, that if lost, stolen, or published in the media could have damaging consequences to the organisation, but is not subject to a heightened threat profile.

If an individual or sender perceives that the release of the information may cause harm, an OFFICIAL classification must be used. Also, if information has not been classified it is assumed to be OFFICIAL.

Examples of OFFICIAL information include:

- The majority of GMP information and services, including most policy development, service delivery, legal advice, personal data that is required to be protected under the DPA, contracts, statistics, finance, intellectual property, and administrative data.
- Personal information where compromise would risk, but not directly threaten, safety of police officers and police staff, other organisations, or the public.
- Information about investigations and civil or criminal proceedings that could compromise public protection or law enforcement activities, or prejudice court cases.

### 5.2.2 OFFICIAL-SENSITIVE

In some instances where the information is higher risk (without being a SECRET classification), for example, if incorrect disclosure or loss could reasonably be expected to significantly threaten safety or compromise an investigation, or where the 'need to know' basis must be enforced; the OFFICIAL-SENSITIVE caveat must be used, and Handling Rules must be annotated e.g. OFFICIAL-SENSITIVE local force only.

The use of OFFICIAL-SENSITIVE should be used by exception, and in limited circumstances where there is a clear and justifiable requirement to reinforce the 'need to know' basis. OFFICIAL-SENSITIVE should be used where a compromise or loss could have damaging consequences for an individual (or group of individuals), an organisation, or for the Force.

Where the OFFICIAL-SENSITIVE classification is used, a "Handling Rule" must also be used.

Documents may often contain information of varying classifications and should be classified in accordance with the highest level of classification that may apply to all or part of the document. For example, if only a small part of the document is OFFICIAL-SENSITIVE then the whole document is to be treated as OFFICIAL-SENSITIVE.

### 5.2.3 SECRET Classification

The majority of GMP staff will not work with SECRET or TOP-SECRET information.

The SECRET classification relates to very sensitive information that justifies heightened protective measures to defend against determined and highly capable threats. Examples include investigating reports of serious organised crime or intelligence operations

SECRET classification relates to information that:

- Threatens life directly,
- Would seriously prejudice public order,
- Threatens an individual's security or liberty, and/or
- Causes serious damage to the continuing effectiveness of highly valuable security or intelligence operations.

### 5.2.4 TOP-SECRET Classification

TOP-SECRET relates to the most sensitive information requiring the highest levels of protection from the most serious threats. This includes information where compromise could cause widespread loss of life, or else threaten the security or economic wellbeing of the country or friendly nations.

TOP-SECRET classification relates to the loss of information that would:

- Directly threaten the stability of the UK,
- Lead to widespread loss of life, and/or
- Cause exceptional grave damage to the continuing effectiveness of extremely valuable security or intelligence operations.

## 5.3 Handling Rules

In some instances where the information poses a higher risk than OFFICIAL, but a lower risk than SECRET then Handling Instructions must be adopted (see 5.3). For example, if disclosure or loss could reasonably be expected to significantly threaten safety or significantly compromise an investigation, or where the 'need to know' basis must be enforced, then the Handling Instruction of OFFICIAL-SENSITIVE must be used along with a Descriptor.

When using the OFFICIAL-SENSITIVE handling rule, the author must always use a Descriptor. Outlook emails and the M365 Office suite have been updated in line with this procedure and it is the responsibility of the author to select the correct label for each document and email (the default is always set at OFFICIAL). In M365 the Security Classification is called a Sensitivity Label and the classification can be selected by clicking on the drop-down box of the Sensitivity Icon on the banner of each application.


## 5.4 Descriptors

Descriptors are used to identify certain categories of sensitive information with the OFFICIAL-SENSITIVE handling instruction. This instruction must only be used with an accompanying Descriptor and not on its own.

What the handling rules and Descriptors mean:

OFFICIAL-SENSITIVE Custom Protection

- The content should be encrypted to restrict access based on user defined permissions. Use only when you need to ensure the content can be viewed by a specific set of users

OFFICIAL-SENSTIVE Protective Marking Only

- No user access restrictions or encryption. For use ONLY when the content must be shared with people who cannot open encrypted content

OFFICIAL-SENSITIVE Local Force Only

- Encrypt the content restricting access to users in GMP only. Use to ensure the content can ONLY be viewed by people in GMP

OFFICIAL-SENSITIVE UK Policing Only

- Encrypt the content restricting access to users from UK police forces only. Use to ensure the content can ONLY be viewed by people in GMP and any other federated Police Force

## 5.5 Sending Email

When sending emails, the default marking is OFFICIAL, however there is the option to choose OFFICIAL-SENSITIVE and the correct Descriptor (as outlined above).

Items with an OFFICIAL classification that contain information or sensitive operational information, or PD and SD/SCD must not be transmitted by insecure email (i.e., from, or to, an email address without one of the below email address domains).

All OFFICAL-SENSITIVE material, whether it includes PD or not, must not be transmitted by insecure email.

Any SECRET or TOP-SECRET material must not be sent by email at all and should not be stored in personal OneDrive accounts, on SharePoint sites, in MS Teams or on other non-policing systems.

GMPs list of approved and trusted (secure) email addresses include:

- gov.scot
- gov.wales
- parliament.uk
- llyw.cymru
- mod.uk
- nhs.uk
- gov.uk
- police.uk

Examples of insecure email addresses are:

- yahoo.co.uk
- outlook.com
- Hotmail.com
- Gmail.com
- Other business and personal email addresses

Internal emai [redacted] is also considered secure, as information sent always remains within GMPs boundaries. However, care should be taken with the use of 'reply to all', where you should ensure that your recipients are the named individuals you wish to contact.

Other security precautions can be taken when a trusted email address is not possible. If no secure email address is available, then encryption or suitable password protection of attached documents must be used.

If there is an urgent requirement to communicate information using inadequate security, the operational urgency, and the need for the manner of communication must be weighed against the risk of a confidentiality/security breach (for which the Force may be held accountable).

For further information regarding email transmission of information with the OFFICIAL classification, and for information with the OFFICIAL-SENSITIVE classification, detailed security requirements can be found in Appendix A.

### 5.6 Storage and Physical Security

In addition to the correct labelling of any information, users must also consider any handling and storage implications associated with the new classifications.

Users should also consider how any information is transferred or moved throughout the organisation or other agency. The requirements are listed in Appendix A.

## 6. Associated Documents

Government Security Classifications - GOV.UK (www.gov.uk)
Appropriate Use of Electronic Communications and Information Systems Procedure
Data Protection Act 2018
Data Protection Policy and Procedure
Freedom of Information Act

## 7. Statutory Compliance & Consultation

### 7.1 Statutory Compliance

#### 7.1.1 Equality Act (2010)

This document applies equally to all police officers, irrespective of any of the protective characteristics. No potential adverse impacts for any protected group under the Equality Act have been identified.

#### 7.1.2 The UK General Data Protection Regulation (GDPR) and Data Protection Act (2018)

GMP has a duty to ensure, so far as is possible, that all officers and staff comply with the provisions of the UK GDPR and the DPA, particularly relating to their access to, and dissemination of, a wide variety of PD and intelligence.

This policy and procedure has been assessed for compliance by the Information Compliance and Records Management Unit (ICRMU) and is considered to be compliant with the legislation. It should be read in conjunction with GMP's Data Protection Policy and Procedure.

[redacted]

#### 7.1.3 Freedom of Information Act (2000)

This policy and procedure is deemed suitable for disclosure under the FOI.

[redacted]

### 7.2 Consultation

The following branches/individuals have been consulted with in relation to this policy and procedure.

[redacted]

| [redacted] | [redacted] |
| --- | --- |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |

## 8. Appendices

GREATER MANCHESTER POLICE

# Retention and Disposal of Records

## Policy & Procedure

**April 2024**

**DATE THIS VERSION OF THE POLICY & PROCEDURE IMPLEMENTED:** April 2024

**DATE NEXT REVIEW IS DUE:** April 2025

**CHIEF OFFICER SPONSOR:** [redacted]

**POLICY & PROCEDURE OWNER:** [redacted], [redacted]

**POLICY & PROCEDURE AUTHOR:** [redacted]

**APPROVED BY:** [redacted]

**GOVERNMENT SECURITY CLASSIFICATION:** Official

**IS THE POLICY & PROCEDURE NEW OR REVISED:** New

| VERSION NO | DATE | SUMMARY OF CHANGES | AUTHOR(S) | [redacted] |
|---|---|---|---|---|
| 1.0 | 04/04/24 | This policy and procedure replaces both V1.3 Retention and Disposal of Policing Records Policy and V7.3 the Retention and Disposal of Non-Policing Records Policy. | [redacted] | 24/14 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Table of Contents

# 1. Policy Statement

Greater Manchester Police (GMP) should only retain records for an appropriate amount of time as stated in the Code of Practice on the Management of Policing Information (MOPI 2005), the Data Protection Act (DPA 2018) and other relevant legislation. The length of a retention period varies and is based on the record's business purpose, legislative, statutory, and best practice requirements. This applies to both physical and digital records.

GMP is committed to ensuring only records with historical information/research value are retained post the retention period of a record. Once a record's retention period is completed, it should be appraised to determine whether it holds any ongoing value for the organisation; if it does not then the record will be disposed.

When applying retention periods, appraisal decisions and disposal methods, GMP will align with national best practices. The benefit of aligning GMP with national policing standards is as follows:

- Information can be managed in a consistent and compliant manner.
- GMP can be confident about disposing of records when it is appropriate to do so.
- GMP is compliant with legislation such as the Data Protection Act 2018, which prohibits the storage of personal data for longer than necessary.

## 1.1 Aims

The aim of this policy and procedure is to provide GMP officers and staff with process regarding the retention and disposal of both policing and non-policing records which are acquired, created, handled, shared and stored by GMP.

A further aim of this policy and procedure is to provide a clear process for GMP officers and staff who gather, handle and store data generated/acquired from the Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 (IPA) in a safe and secure manner.

# 2. Scope

This policy and procedure applies to all of GMP's records and data, regardless of format and the information they contain. It applies to all employees of GMP: officers and staff, contractors, consultants and secondees who have access to records, wherever these records may be located.

GMP are responsible for appropriate mechanisms and governance for the sharing of information – this includes direction to third parties about their responsibilities. For more information, you should refer to the [redacted]

# 3. Roles & Responsibilities

| | |
|---|---|
| **All officers and staff** | Should be aware of their responsibilities under the legislation and in relation to the handling and processing of personal data. Compliance with DPA 2018 and UK General Data Protection Regulations (UK GDPR) is the responsibility of all employees who process personal data.<br><br>It is the responsibility of all GMP officers and staff to ensure all records under their care are disposed of in a timely manner when there is no longer a requirement for retention.<br><br>It is the responsibility of each officer and staff member to apply the appropriate retention period and arrange suitable disposal when required to both the physical and digital records under their authority. |
| **Data Controller** | The Chief Constable of GMP is the notified Data Controller for the purposes of the DPA 2018 and UK GDPR. As such, they are obliged to ensure that GMP handles all personal data in accordance with Data Protection legislation. |
| **Force Data Protection Officer** | This is the role who is the lead on data protection policy and procedure; assists with monitoring internal compliance, informing and advising on data protection obligations, providing advice regarding Data Protection Impact Assessments (DPIAs) and acts as a contact point for the supervisory authority, the Information Commissioner (ICO). |
| **Information Asset Owner (IAO)** | The owner of an Information Asset is responsible for ensuring that the asset is managed appropriately, in compliance with the legislation, to meet the requirements of the organisation, and any risks and opportunities are monitored. |
| **Information Asset Administrator (IAA)** | Nominated by the IAO and is responsible for the day-to-day management of the information asset and its entry in the ROPA. |
| **Information Compliance and Records Management Unit** | This unit comprises the data protection subject matter experts for the Force. A list of contacts is available on the intranet. The Unit is responsible for:<br>• Handling requests for information under: UK GDPR and DPA 2018 (Article 15 UK GDPR and Section 45 DPA – subject access); Freedom of Information Act (FOI), Environmental Information Regulations (EIR); from insurance companies under the ACPO/ABI agreement and the Criminal Injuries Compensation Authority (CICA).<br>• Advising on statutory compliance for all business processes and personal data disclosures to other organisations: review internal personal data breaches; review any requests for data held by GMP to be deleted or corrected by data subjects; handling data protection complaints from the ICO and data subjects; review DPIAs; develop information sharing and data processing agreements/contracts with third party processors; undertaking audits of Force systems; and promoting good practice. |

| | |
|---|---|
| **Information Security** | The Information Security Team manage, advise on and assess information security risks and issues. |
| **Professional Standards Branch** | Investigate potential misconduct, including potential breaches of data protection and information security. |
| **Records Management** | Controlling a record throughout each stage of the record's lifecycle to ensure it can be used as authoritative evidence. |
| **Senior Information Risk Owner** | This role has responsibility for managing risk associated with information compliance matters relating to information. |

## 4. Terms and Definitions

| | |
|---|---|
| **Archive** | Records which have been selected for permanent preservation due to their continued value.<br>*NOTE: records which have not been subject to a retention period and appraisal decisions are not archived records.* |
| **Appraisal** | The process of evaluating a record to determine whether the record has ongoing value to the organisation once the record has fulfilled its business needs and requirements for accountability. |
| **CD** | Communications Data |
| **DeepStore** | Off-site storage company used for the long-term storage and preservation of records and exhibits. |
| **Disposal** | The deletion or destruction of records once the minimum retention period is complete and the record has no further value in accordance with the relevant Force policies. |
| **DPA** | Data Protection Act |
| **DPIA** | Data Protection Impact Assessment |
| **UK GDPR** | UK General Data Protection Regulation |
| **GSC** | Government Security Classification |
| **IPA (2016)** | Investigatory Powers Act |
| **IPDA** | Investigatory Powers Data Assurance |
| **MoPI** | Management of Policing Information |
| **NPCC** | National Police Chiefs' Council |
| **PNLD** | Police National Legal Database |
| **Record** | Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business (BS ISO 15489-1:2016). |
| **Record Lifecycle** | As records are living documents, the record lifecycle refers to the different stages of a record throughout its life. |
| **Retention Period** | The period of time a record is kept for in order to meet its organisational, legislative and statutory requirements. |
| **RIPA (2000)** | Regulation of Investigatory Powers Act 2000. |

# 5. Procedure

## 5.1 Police Corporate Information

Police corporate information is information that is processed to enable the discharge of police services, such as financial information, policies and procedures, and information relating to employees, such as personnel and disciplinary records.

GMP is committed to upholding the standard outlined by those requirements when applying retention and disposal decision to records produced, used, and stored by the organisation. Therefore, it is of paramount importance that records are retained in-line with legislative, statutory, and best practice standards. All officers and staff must consult and follow the best practices outlined by the National Police Chiefs' Council **National Guidance on the Minimum Standards for the Retention and Disposal of Police Records** when applying retention and disposal decisions to police corporate information. In addition to this, all police corporate information is subject to the **Police Information and Records Management Code of Practice** and should always be consulted when making retention decisions.

## 5.2 Police Operational Information

Police operational information is information that is recorded for a policing purpose, mainly (but not exclusively) for: protecting life and property; preserving order; preventing the commission of offences; bringing offenders to justice;and any other police duty or responsibility arising from common or statute law.

It should be noted that the range of policing purposes is wider than the following definition of law enforcement purpose, which is provided for in section 31 of Part 3 of the DPA 2018: "*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.*"

It is GMP's policy to use the retention periods and disposal decisions outlined by the **Police Information and Records Management Code of Practice**, when applying retention and disposal decisions to all policing records acquired, produced, handled and stored by GMP.

| Review Group | Example of Offence and Record Type | Action | Rationale |
|---|---|---|---|
| Group 1 – serious offences and public protection matters | Multi-agency public protection arrangements (MAPPA) managed offenders.<br><br>Offences specified in the Sentencing Act 2020 Schedule 18 which carry a maximum sentence of 10 years or more. | Having considered the retention criteria detailed, you may retain until the nominal has reached **100 years** of age, then carry out a manual review.<br><br>Review every 10 years to ensure accuracy and necessity. | This category poses the highest possible risk of harm to the public. |

| | | | |
|---|---|---|---|
| | Potentially dangerous people. | | |
| Group 2 – other sexual and violent offences | Sexual offences listed in Schedule 3 of the Sexual Offences Act 2003.<br><br>Violent offences specified in the Home Office Counting Rules for recorded crime and the National Crime Recording Standard.<br><br>This group also includes offences specified in Schedule 18 of the Sentencing Act 2020, which are not group 1 offences, i.e., carry a maximum sentence of less than 10 years.<br><br>Other serious offences are recorded as such on the **Police National Legal Database** (PNLD). | Review after an initial 10-year clear period.<br><br>If the subject is deemed to pose a high risk of harm, retain and review after a further 10-year clear period. | National Retention Assessment Criteria (NRAC) |
| Group 3 – all other offences. | All other offences. | Retain for an initial 6-year clear period, followed by subsequent 5-year clear period reviews.<br><br>Either review and risk assess after a 6-year clear period or carry out time-based disposal depending on Force Policy. | Lower risk of harm.<br><br>Forces must balance the risk posed by this group with the burden or reviewing. |

To ensure the records are stored and appraised in line with the guidance set out in the Police Information and Records Management Code of Practice, all officers and staff must:

- Ensure the police information group for the offence is correct, in order to apply the correct retention schedule. This must be verified prior to applying a retention period.

The group that an offence belongs to can be verified using the PNLD. Users need to register their details to gain full access to the database.

- Not retain records beyond the retention periods outlined in this policy and procedure.

## 5.3 Record Disposal

GMP is dedicated to upholding the data protection principles; all officers and staff should dispose of all records in a timely manner when the retention period is completed as outlined in this policy. UK GDPR states that personal data must be "*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*".

All records should be disposed of in line with the practices and principles outlined in the **Police Information and Records Management Code of Practice**.

### 5.3.1 Record Disposal Accountability

[redacted]

Ultimately, the accountability for appropriate record disposal rests with the Data Controller for GMP, the Chief Constable, but this responsibility is delegated to the Information Asset Owners in respect of their individual areas of business.

[redacted]

## 5.4 Investigatory Powers Data Assurance

GMP is committed to the safeguarding of data collected using the Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 (IPA) codes of practice. All officers and staff who handle data generated using investigatory powers should use the processes set out in this policy, with supplementary guidance and support on the Investigatory Powers Data Assurance (IPDA Intranet).

[redacted]

[redacted]

### 5.4.1 Safeguarding of Covert Data

When safeguarding data acquired and generated by the acquisition of covert data (CD) and the use of DSA, officers and staff should follow the codes of practice and the policies produced by the National Police Chiefs' Council (NPCC). More information can be found [redacted].

#### 5.4.1.1 Secure Storage of Data

In order to ensure all data which is acquired or generated using an investigatory power remains secure, officers and staff must:

- Ensure data is consistently stored within a dedicated and secure operational folder.
- Exercise care when permitting access to data, so that only relevant operational staff can access it. Appropriate access controls (passwords etc.) should be applied accordingly.

#### 5.4.1.2 Communications Data

It is the responsibility of the officer or member of police staff who is applying for CD (the applicant) to ensure that the data is stored and handled securely. On occasion, responsibility for safeguarding the data may be transferred in certain circumstances, for example in a complex investigation the Senior Investigating Officer (SIO) may take responsibility for all data acquired during an investigation or may appoint a suitable officer to take responsibility of data.

To ensure CD is stored securely, the applicant should ensure that it is initially acquired and stored within the [redacted], a safe and secure system that has been approved for the storage of CD and is administered by the Communications Data Investigation Unit (CDIU). The applicant should then copy all data in all formats, including applications and authorisations, from the [redacted] immediately into a secure operational folder, with appropriate access controls in place to ensure there is restricted access to necessary operational staff only.

Frequently, there is an operational requirement for CD to be included in reports, analysed using software or shared with other agencies and partners. In such circumstances, officers and staff should only transfer/send CD from secure GMP approved Information Services (IS) systems. This will safeguard the data from data breaches. For further information regarding the security of data, you should refer to the [redacted]

### 5.4.2 Directed Surveillance Authorities (DSA)

It is the responsibility of the applicant for a DSA to ensure that the data is stored and handled securely. Responsibility for the data may be transferred in certain circumstances e.g., in a complex investigation the SIO may take responsibility for all data acquired or may appoint a suitable officer to take responsibility of data.

To support the safe and secure storage of data generated or acquired using an investigatory power, the applicant must ensure that data is always stored within a secure operational folder, with restricted access to operational staff only. For example, in the "[redacted]

Frequently, there is an operational requirement for data acquired using surveillance to be included in reports, analysed using software or shared with other agencies and partners. In such circumstances, officers and staff must ensure the data is transferred via a secure GMP-approved [redacted] In the case where data is copied into a paper document, that document must always be held securely in line with the electronic transfer of data and its Government Security Classification (GSC). For further information regarding the security of documents, you should refer to the [redacted]

All data handled and acquired via the use of investigatory powers by officers and staff must always be:

- Protected from unauthorised access – files, folders and electronic documents containing data are password protected.
- Only copied in circumstances limited to that which is necessary for a policing purpose e.g., analysis of complex data, inclusion of the data in a prosecution file or a report submitted to the Crown Prosecution Service (CPS).
- Only shared with other agencies for a lawful policing purpose – all data shared outside of GMP will contain handling instructions providing clear direction to the recipient of the requirement to store the data securely and prevent unauthorised access.

### 5.4.3 Retention, Review and Disposal of Data

Every officer and staff member is responsible for the safeguarding of material obtained through the use of covert powers, and assessing compliance with the relevant sections of the Codes of Practice for the Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 (IPA).

The safeguarding of covert data is a legislative requirement and therefore it is the responsibility of each officer and staff member to continually review all data held. When the requirement to retain the data ceases to exist, all data in all formats held on GMP-approved [redacted] etc., should be disposed of. As such, officers and staff must:

- Only retain data where there is a lawful policing requirement and power to do so.
- Conduct regular reviews to ensure there is an ongoing requirement to retain data.
- Have a process in place to routinely dispose of data when the requirement to retain ceases.

Finally, GMP recognises the importance of adhering to the requirements of the Criminal Procedure and Investigation Act 1996 and Management of Policing Information 2005. All officers and staff members should always consider both when deciding how long data should be retained for.

## 6. Associated Documents

- [redacted]

- [redacted]

# 7. Statutory Compliance & Consultation

## 7.1 Statutory Compliance

This policy complies with the following legislation:

- Criminal Procedures and Investigations Act 1996
- Data Protection Act 2018 and UK GDPR
- Investigatory Powers Act 2016
- Regulation of Investigatory Powers Act 2000

### 7.1.1 Equality Act (2010)

This policy and procedure will affect both GMP officers and staff as well as our wider communities as it covers all records produced, handled and stored by GMP. This document will affect those groups positively as it sets out how GMP will comply with relevant legislation and ensure data is dealt with in a safe and secure manner, thus complying with data rights. This policy ensures that any person with protected characteristics is not discriminated against as records will be managed in line with national policing standards and applied to all record types.

### 7.1.2 The UK General Data Protection Regulation (UK GDPR) and Data Protection Act (2018)

Greater Manchester Police has a duty to ensure, so far as is possible, that all staff comply with the provisions of the UK GDPR and the Data Protection Act 2018, particularly relating to their access to, and dissemination of, a wide variety of personal information and intelligence.

This policy is compliant with GMP's responsibility under the Data Protection Act (2018).

### 7.1.3 Freedom of Information Act (2000)

This policy shall be subject to disclosure under the provisions of FOI and GMP shall be obliged to consider its disclosure under the FOI act, and associated documents, to anyone requesting them under Freedom of Information.

However, any requests for its disclosure should be directed through the Information Compliance and Records Management Unit via the Freedom of Information mailbox after reviewing previously published FOI via GMP's Publication Scheme.

## 7.2 Consultation

The following departments have been consulted throughout the development of this policy and have provided the following feedback.

| | |
|---|---|
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |

## 8. Appendices

None