Information Compliance and Records Management Unit (ICRMU)
Information Management Branch

Date: 10/05/2024
Our ref: 01/FOI/24/012458/L

FREEDOM OF INFORMATION REQUEST REFERENCE NO: 01/FOI/24/012458/L

I write in connection with your request for information dated 12/04/2024, received by Greater Manchester Police (GMP) for the following information:

Please can you inform which department(s) manage requests for disclosure form the parole board, and provide copies of any relevant local policies that deal with this process?

Result of Searches

Following receipt of your request searches were conducted within Greater Manchester Police (GMP) to locate information relevant to your request. I can confirm that the information you have requested is held by GMP. However, I am not obliged to supply you with all of 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. The information you have requested is exempt from disclosure by virtue of the following exemption: **Section 40(2) – Personal Information.**

Where redactions occur in the attached Information Sharing Policy and Procedure, 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.

In accordance with the Section 17 of the Freedom of Information Act 2000, this letter acts as a Refusal Notice.

The Criminal Justice Unit manage requests for disclosure from the Parole Board.

Please find attached a redacted copy of GMP's Information Sharing Policy and Procedure.

Information Sharing

Policy & Procedure

Greater Manchester Police

January 2023

POLICY & PROCEDURE IMPLEMENTED: January 2023

REVIEW DATE: January 2024

POLICY & PROCEDURE OWNER: [redacted], Head of Information Management

APPROVED BY: [redacted]

IS THE POLICY & PROCEDURE NEW OR REVISED? Revised

GOVERNMENT SECURITY CLASSIFICATION: Official

VERSION NO	DATE	SUMMARY OF CHANGES	AUTHOR(S)
1.0	13/12/2012	Replaces Information Sharing Policy from 2008, revised in line with Authorised Professional Practice.	[redacted]
2.0	07/01/2014	Replaces appendices with hyperlinks to SharePoint, update contacts, document revised in line with new policy format	[redacted]
2.1	15/07/2014	Reformatting content, addition of 7. Information Security, 1.1 Aims and 1.2 Benefits of information sharing	[redacted]
2.2	27/10/2014	Reformatting	[redacted]
2.3	04/11/2014	Realignment of content to match template contents page, addition of 5.8	[redacted]
2.4	18/11/2014	Updates to URLs and links to policies	[redacted]
2.5	01/11/2022	Moved to Policy and Procedure template, updated terminology and legislation, content reviewed, and all links updated.	[redacted]

Table of Contents

1. Policy Statement

Effective policing is dependent on efficient control of police information which includes communicating and sharing information with a wide range of partners, either in a one off scenario or in on-going relationships, where the sharing will help to achieve a common objective of benefit to both parties.

The purpose of this policy and procedure is to ensure that the sharing of police information is carried out in a lawful manner that is fit for purpose, taking into account the necessity, adequacy, relevancy, accuracy, proportionality and timely provision of the information.

This policy and procedure takes full account of the guidance contained in Authorised Professional Practice (APP) – Information Management.

1.1 Aims

In order to fulfil its strategic aim, GMP will:

- Actively seek opportunities to share personal and non-personal information with partners.
- Seek to engage our partners in the information management debate and reach agreement on information sharing where possible.
- Ensure that information sharing takes place in a lawful manner by establishing a policing purpose or other legal gateway prior to disclosure and ensure that the necessity and proportionality of the disclosure are considered.
- Conduct a Data Protection Impact Assessment (DPIA) to assist the Force in making the correct information sharing decision and implement safeguards which have real benefit to the information sharing initiative and the security of shared data.
- Assess each request for information to be shared on a case-by-case basis and make an informed decision about whether or not to disclose.
- Put Information Sharing Agreements (ISAs) in place when there is a frequent and continuing need to share police information. Such protocols will be agreed on the basis that partners will only use police data for lawful purposes, maintain security and confidentiality of police information and formalise the information sharing processes and procedures. These agreements shall be reviewed in accordance with the APP – Information Management, Sharing Police Information section to ensure that they are still fit for purpose and of benefit to the initiative.
- Publish current ISAs to the Force via the intranet to assist those receiving information sharing requests to verify that an organisation is a signed-up partner of GMP.
- Ensure that when information is received from other agencies (e.g. local authorities), its reliability and context is understood before it is recorded on GMP systems or made use of. Methods will also be devised to update that information, where necessary, when it is changed on the source system.
- With advice, guidance, templates and full support from the Information Compliance and Records Management Unit (ICRMU), assist in progressing information sharing initiatives.
- Ensure that individuals are not permitted access to, or use of, information unless they can demonstrate a legitimate reason for such access, and an understanding of how

the information should be handled in accordance with its protective marking under Government Security Classifications (GSC).
- Identify single points of contact (SPOCs) for information sharing initiatives and provide them with clear and useful support and guidance to assist them in their information sharing role.

1.2 Benefits of Information Sharing

The implementation of this policy and procedure within GMP will have the following benefits:
- Assist operational policing by creating two-way information sharing processes that enable information, which will assist with our policing obligations, to be shared and received in a lawful and convenient manner.
- Help to ensure that all disclosures of police information are made on a sound and consistent basis, whether in on-going relationships or one-off scenarios.
- Allow for the efficient and consistent production of useful ISAs to formalise the sharing process where police information is being shared on a regular basis.
- Ensure that ISAs are reviewed so that they are fit for purpose and that all stakeholders are working to the correct version of the document.
- Increase expertise, professionalism and understanding of the process of sharing information and putting ISAs in place.
- Increase openness and transparency among partners, which in turn builds confidence and trust in the police service.
- Provide protection to each of the partners involved in the information sharing initiative, in terms of information security, use of shared data and indemnity.

2. Scope

This policy and procedure applies to information processed for a policing purpose by GMP and applies to any verbal/oral, written, electronic, photographic and paper based information.

For the purpose of this document, the term ‘information sharing’ includes dissemination and disclosure.

This policy and procedure does not cover the Disclosure and Baring Service’s (DBS’s) Quality Assurance Framework or the sharing of material as defined in the Criminal Procedure and Investigations Act (CPIA) 1996.

This policy and procedure does not prevent the sharing of information between police forces for a policing purpose, nor does it prevent the capability for urgent sharing of information to safeguard children and other vulnerable people.

3. Roles & Responsibilities

The following staff members have direct involvement in information sharing:

- ACO (Assistant Chief Officer) Resources: Force strategic lead and authorising officer on behalf of GMP.
- Data Protection Officer (DPO): Responsible for reviewing, signing off and providing advice on information sharing.
- ICRMU Manager: Day to day supervision of the ICRMU.
- Information Compliance and Records Management Officers: Responsible for monitoring compliance and day to day issues involving information sharing.
- All officers, staff, and contractors: To be aware of their responsibilities under the Data Protection Act 2018 and in relation to information sharing.

4. Terms and Definitions

Below is a list of terms and definitions used throughout this document:

ACO	Assistant Chief Officer
APP	Authorised Professional Practice
CPIA	Criminal Procedure and Investigations Act (1996)
DBS	Disclosure and Barring Service
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
GDPR	General Data Protection Regulation
GSC	Government Security Classification
ICRMU	Information Compliance and Records Management Unit
ISA	Information Sharing Agreement
SPOC	Single Point of Contact

5. Procedure

Due to the personal and sensitive nature of police information, statutory obligations under the Data Protection Act 2018 must be met when processing information at all stages of its lifecycle.

To achieve this, we must demonstrate a consistent approach across the organisation when sharing police information with partners and agencies. The procedure for establishing an ISA involves an initial feasibility assessment to determine the need and legal basis for sharing information with a third party. To assist with this an Information Sharing Flowchart has been produced.

This procedure takes you through a step by step process for implementing information sharing initiatives in a lawful manner.

5.1 Policing Purposes

Information processed by GMP, including intelligence and personal data, is obtained and recorded for a policing purpose(s). To lawfully share police information, a policing purpose must be identified. Policing purposes for processing information are:

- Protecting life and property,
- Preserving order,
- Preventing the commission of offences,
- Bringing offenders to justice, and
- Any duty or responsibility of the police arising from common or statute law.

5.2 Legal Gateways

Information must only be shared if a legal gateway such as, statutory obligation, statutory power or a policing purpose (common law), has been identified. Each of these is also explained in the APP – Information Management. Some typical examples of common law, statutory obligations and powers are set out below. For further details see the Information Sharing Agreement Guidance Document and/or contact the ICRMU.

There is no general statutory obligation or power to share information. Some Acts of Parliament give public bodies express statutory powers to share information; these are often referred to as 'legal gateways' and are enacted to enable the sharing of information between certain partners for particular purposes. These gateways may be mandatory or permissive.

5.2.1 Statutory Obligation

A statutory obligation is a mandatory gateway where the information must be disclosed as instructed by legislation, subject to ensuring that the information shared is adequate, relevant and not excessive for the purpose. Examples include:

- The Audit Commission Act 1998, as amended by the Serious Crime Act 2007, Section 32B places an obligation on public authorities to share employees' personal data with the National Fraud Initiative.
- The Education Act 2002, Section 175 places an obligation on public authorities to share information with schools and local authorities to protect the welfare of children.
- Court orders place a legal obligation on an organisation to disclose the described information with the specified agency.

5.2.2 Statutory Power

A statutory power is a permissive legal gateway where the information may be disclosed. The organisation holding the information can make a decision whether they wish to share the information; the legislation provides the organisation with the legal power to make the disclosure. Examples include:

- The Data Protection Act 2018, Schedule 2 Part 1 (2) exempts organisations from the non-disclosure provisions of the Act where the information sharing is in the interests of preventing and detecting crime, and/or the apprehension and prosecution of offenders, where failure to disclose would prejudice those purposes. Schedule 2 Part

1 (5) exempts personal data from the non-disclosure provisions of the Act where it is required by or under any enactment and this also provides the same exemption where the information is required in connection with legal proceedings.

- The Crime and Disorder Act 1998, Section 17 places an obligation on public authorities to co-operate with each other, however this does not specifically refer to information sharing. Section 115 gives a legal power to share information in the interest of preventing and detecting crime and/or disorder.
- Immigration and Asylum Act 1999, Section 20 gives the police a legal power to disclose information to the Secretary of State (the Border and Immigration Agency) for immigration purposes.
- Anti-Terrorism, Crime and Security Act 2001, Section 17 (2) allows public authorities to disclose information to assist with criminal investigations and/or proceedings where the disclosure is proportionate.

5.2.3 Common Law

This applies to all cases where there is a pressing social need to share information to support a policing purpose and none of the above applies. When common law is used as the justification, a thorough data protection assessment should be conducted. The necessity and the proportionality of the disclosure must also be considered.

Administrative convenience will not necessitate the disclosure of information. For example, if the information can be obtained from another source which would not cause prejudice to an individual then this source should be the preferred option. Only enough information should be disclosed in order to achieve the purpose. Each decision must be made on a case-by-case basis and not according to a blanket policy. The assessment must also take into account the source of the information and any possible onward disclosure.

The guidance on the APP – Information Management Sharing Information and Common Law Section requires any decision about the disclosure of details of sex offenders to schools or other educational institutions to be made by an officer of chief officer rank.

When deciding whether to share information using a statutory power or common law duty of disclosure a guide to conducting a DPIA should be completed. This involves assessing any benefits that the information sharing might bring to society or individuals against any negative effects, such as an erosion of personal privacy, or the likelihood of damage, distress or embarrassment being caused to individuals. Where potential negative impacts are identified, measures should be considered to help avoid or minimise the risk of any detriment being caused. In both cases the worst scenario should be considered.

5.3 Information Security

Wherever possible all efforts must be made to share anonymised data, however when a decision has been made to share personal or sensitive information, the means by which information is to be shared must be adequately secure to safeguard the information from accidental loss damage or destruction to ensure information integrity.

Methods by which you may secure information include (but are not limited to) some of the following:

- Password protection,
- Courier/hand delivered/collection,
- Vetting of non-police personnel in respect of third party information processing e.g. data processing agreement, research agreements etc.,
- Encryption,
- Data anonymisation,
- Secure email,
- Restricted user access account, or
- Physical site security.

If you are unsure of the level of security required for the information you want to share, please consult the ICRMU.

5.4 Privacy Policies

When information about an individual is to be shared that would not be within that person's legitimate expectations, a privacy policy should be provided. The notice should give a comprehensive and accurate description of what information is being shared, the purpose for the information sharing and details of whom it is being shared with.

It is good practice to draft an individual privacy policy for each information sharing initiative. For further information and sample templates refer to the ISA guidance document, and the ISA Template.

There are cases where it is legitimate to share information without a person's consent or knowledge; this might be the case where a failure to share information about a parent's lifestyle would put a child at risk or where information sharing is necessary to safeguard public safety in an emergency situation. There are also other situations where information should be shared without the individual's knowledge, for example, where doing so would prejudice a particular investigation.

5.5 One-off Information Sharing

Where the decision to share information is a one-off, GMP will ensure that a thorough risk assessment is undertaken considering the following issues:

- Who is making the request for information?
- What is the protective marking of the information under GSC?
- Is the information personal data? (Can a lawful basis be satisfied under Article 6 UK General Data Protection Regulation (GDPR)?)
- Is the information special category data? (Can a lawful basis be satisfied under Article 9 UK GDPR?)
- Has a legal gateway or policing purpose for sharing the information been established?
- In what format is the information required? (Can it be further disseminated)

- Methods for safeguarding the information shared.

All information sharing requests will be owned by the district or branch making the disclosure and the record should be signed by the District or Branch Commander.

Special category data is defined in UK GDPR as categories of data that include information concerning:

- Racial and ethnic origin,
- Political opinions,
- Religious or philosophical beliefs,
- Trade union membership,
- Genetic data,
- Biometric data,
- Data concerning health,
- Data concerning a person's sex life, and
- Data concerning a person's sexual orientation.

Criminal offence data covers a wide range of information about offenders or suspected offenders in the context of criminal activity, allegations, investigations, and proceedings. This information is likely to have an increased potential to cause prejudice to an individual if misused and as such is protected further under the provisions of the Act.

5.6 Information Sharing Agreements

Whenever there is a frequent and continuing need to disclose information to another agency or partner for the same purpose, consideration should be given to establishing an ISA.

Where GMP shares information on a frequent and continuing basis with a partner, either a new ISA must be put in place, or an existing agreement must be reviewed and extended (in accordance with Section 1.1 of this document) where an appropriate one already exists. All such agreements entered into by GMP will comply with APP – Information Management, Sharing Police Information Section.

The first step is to identify an owner for the information sharing initiative, who shall liaise with the ICRMU at the earliest available opportunity to discuss the potential sharing. If the agreement owner has previous experience of drafting ISAs and bringing proposals to fruition, they should draft the first version of the ISA using the ISA Template. The owner should also complete a DPIA and submit these to the ICRMU. If the identified owner does not have this level of experience, they should simply submit the DPIA and a member of the ICRMU would then be allocated to work alongside the agreement owner to assist in the production of an appropriate agreement.

The ICRMU will provide advice and guidance at all stages of the process and be responsible for the quality assurance of the final agreement for data protection, information security and information management compliance purposes. The ICRMU will store and maintain (including change control) all ISAs centrally.

All Force ISAs will be subject to formal Change Control.

Following a risk-based assessment, information sharing within ISAs will be audited on a regular basis by the ICRMU.

All ISAs will be owned by the district or branch which entered into them but will be maintained and stored centrally.

ISAs that have been quality assured will be forwarded by the ICRMU for signing by the DPO.

ISA is a ‘catch-all’ term which shall also include Data Processing Agreements, Information Systems Access Agreements, Research Agreements and Overarching Information Sharing Agreements.

This process is fully described in ISA Guidance Document which provides a step by step guide for establishing and recording ISAs.

5.7 Information Transfer

The main consideration in determining an appropriate method of information transfer is the protective marking of the information to be shared under the GSC. This takes into account the sensitivity and impact of compromise of the information when determining a proportionate level of security to be applied to the information during handling, storage, transfer and disposal.

Appropriate methods of transfer for information up to Confidential GSC Marking can be seen below. If you have a need to transfer information of Secret or Top Secret marking, you should contact the Information Security Manager directly to discuss your requirements.

5.7.1 Paper Records

Paper records are particularly vulnerable in transfer as they cannot be encrypted or password protected in anyway. If they are exposed, they can be read. Consider whether scanning and sending by one of the encrypted means seen below is more appropriate.

Transfer of Records in Person

This is the recommended method of transfer for paper records. By transferring in person you can be positive that the information has reached its intended recipient. It is important that the paper records remain securely within your positive control at all times during transit. Positive control means that you are in complete control of the information.

Post or Courier

This must only be used for ad hoc one off sharing only. The information should be placed into a well-sealed envelope (use of Sellotape recommended) with no protective markings shown on the outside of the envelope. The full address of the recipient should be very clearly

written (computer printed recommended) and displayed. The information should be sent by first class post and using recorded delivery.

Information of Official-Sensitive marking should be placed within two envelopes, each addressed, and the protective marking only shown on the outside of the inner envelope. A return address should be clearly printed on the outer envelope. The information should be sent by special recorded delivery.

Post or courier should not be used to transfer information in a regular and on-going information sharing initiative. Alternative arrangements should be made.

5.7.2 Electronic Records

Use of the following encrypted methods allows electronic records to be transferred efficiently and securely.

Secure E-mail

This can only be used for information up to Official marking only. Secure e-mail probably represents the most efficient and convenient means of transferring information. The following e-mail domains are within the Criminal Justice Extranet and may be used to e-mail information up to Official marking:

- .pnn.police.uk
- .nhs.net
- .gsi.gov.uk
- .cjsm.net
- .gcsx.gov.uk
- .gse.gov.uk
- .gsx.gov.uk
- .scn.gov.uk

The standard e-mail addresses of most of our partners are not secure. You must check that the e-mail address contains one of the above extensions only.

Unless you know exactly who the members of an e-mail group or inbox are and they all have a need to know, send the e-mail to particular recipients only. If a group e-mail or inbox is to be used encrypt the attachment as below and only give the password to those who have a need to know by an alternative means, i.e. telephone call.

Finally, consider how large the files are which are to be transferred. Both outgoing and incoming e-mail rules may block large e-mails and so you may find that your e-mail is quarantined and needs to be approved before reaching its intended recipient. Such quarantine may mean that internal and external systems administrators have access to the information. As such, you should avoid sending e-mails which are likely to trigger these filters.

Encrypted Memory Sticks

These can only be used for information up to Official marking only. Encrypted memory sticks may be obtained by following the procedure for use of USB Memory Sticks documented in the Appropriate Use of Electronic Communications and Information Systems Procedure. The procedure states that USB memory sticks are not to be issued on a permanent basis and as such are not suitable for long term on-going sharing initiatives.

You will be required to choose a password for the USB memory stick, you should familiarise yourself with the Section 5.7.3 of this document before doing this.

The USB memory stick still needs to physically get to the intended recipient so will need to be transferred in person or posted as per the rules seen in Section 5.7.1.

The information should be removed off the USB memory stick once it has been transferred. USB control software will prevent information being written to non-issued encrypted USB memory sticks.

CD ROMS and DVDS

These can only be used for information up to Official marking. Information which has been encrypted could be burnt to a CD ROM or DVD to be transferred, however e-mail is likely to be more convenient means of transferring smaller data files and Encrypted USB memory stick will likely be more convenient for sharing larger data files which would be unsuitable to be e-mailed.

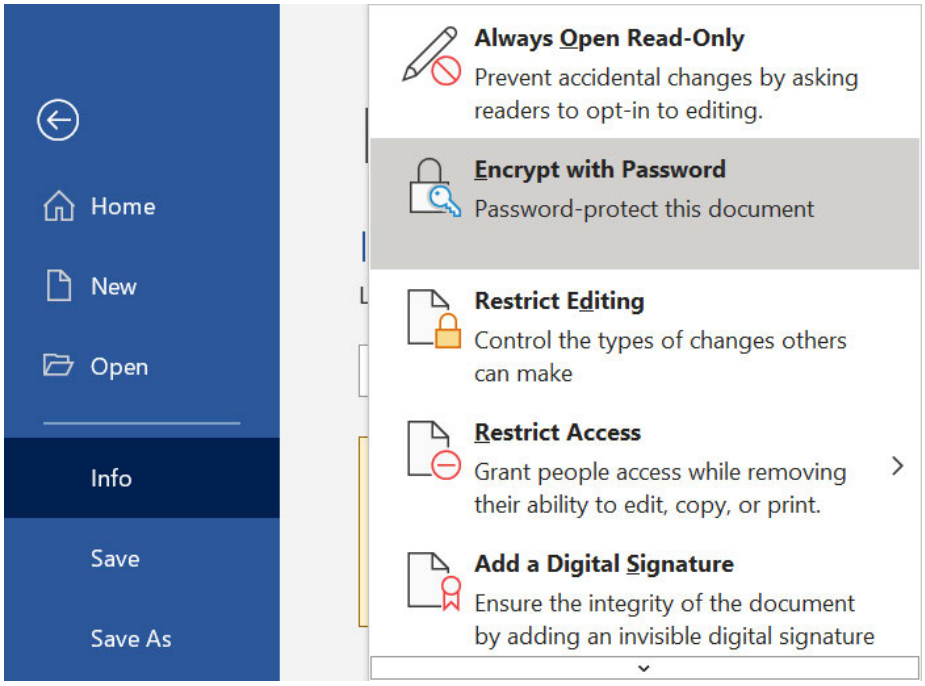
The CD-ROMs still need to physically get to their intended recipient so will need to be transferred in person or posted as per the rules in Section 5.7.1.

5.7.3 Encrypting Information

Encrypting with password

File encryption helps protect your data by encrypting it. Only someone with the right encryption key (such as a password) can decrypt it.

To do this, open your document and click file in the top left-hand corner. Select Info, and then protect document. Select ‘Encrypt with Password’ and enter the password of your choice.



Choosing a password

Use of encrypted memory sticks and encryption both require a password to be chosen. The following instructions from the Appropriate Use of Electronic Communications and Information Systems Procedure must be followed.

The password must consist of:

- At least eight characters;
- Multiple letters and numbers; and
- Multiple upper and lowercase letters.

To make your password more difficult to guess, you must not use:

- Common words that are found in dictionaries (most password cracking devices run a dictionary check first).
- The word “password” or any derivative of the word “password” such as Password12 or Password75.
- Alphabetic, numeric or keyboard sequences such as “Abcdefg34” or “A123456789” or “Qwerty789”
- Consecutive identical characters e.g. “Aabbcc1122”.

Your password should be communicated to the recipient using an alternative means to how the information is to be transferred. For example, if e-mailing an encrypted file or posting an encrypted USB memory stick, telephone the recipient to provide them with the password.

5.7.4 Necessary and Relevant Data Sharing

You should only transfer the right amount of personal information which enables the purpose of the sharing to be achieved. You should not share excessive personal information which is

not necessary and not relevant; doing so will be unlawful and will unnecessarily increase the impact in the information is compromised.

5.8 ISA Change Control

Change control is about ensuring the Force and its partners have a resilient mechanism for checking that they are working to the latest version of the document and that this version has been properly assessed for compliance prior to sign off. This will be accomplished by recording the 'Version Record' of an agreement as seen on the front page of the ISA Template.

When an amendment to the agreement is required, the ICRMU must be notified. The amendments should be made, including updating the version record, and the new agreement's version number should be upgraded sequentially. A record of the latest version of the agreement will be maintained centrally by the ICRMU and stored on the unit's secure SharePoint site.

6. Associated Documents

This document should be read in conjunction with the following:

- Information Security Policy
- Data Protection Impact Assessment
- Data Protection Policy and Procedure
- Personal Data Breach Policy
- APP – Information Management
- Appropriate Use of Electronic Communications and Information Systems Procedure
- Information Sharing Agreement Guidance Document
- Information Sharing Flowchart
- ISA Template

Other reference material includes:

- The Information Commissioner's Information Sharing Code of Practice
- Lord Chancellor's (2002) Code of Practice on the management of records issued under Section 40 of the Freedom of Information Act, 2000.
- College Learn - Information Sharing Agreements under GDPR

7. Statutory Compliance & Consultation

7.1 Statutory Compliance

7.1.1 Equality Act (2010)

This policy has been written with the intention of having a positive effect on diversity and equality and is complaint with the Act. The main intentions of this policy document are to:

- Eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under the Act.
- Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it.
- Foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

The relevant protected characteristics considered are: Age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

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

This policy and procedure has been rigorously assessed for compliance with the seven principles of the Data Protection Act (2018) and the Human Rights Act (1998).

7.1.3 Freedom of Information Act (2000)

This policy and procedure has been rigorously assessed for compliance with the Freedom of Information Act (2000).

7.2 Consultation

Consulted	Comments
IS Branch	Due to the specialised nature of this policy, it has been developed mainly by staff within ICRMU.
Counter Corruption Unit, Professional Standards Branch	
Police Federation – [redacted]	Queries received; no amendments required.
Trade unions (UNISON/GMB)	
Legal Services	
Force Crime & Incident Registrar	
Staff Associations	
Staff Support Networks	Disability Support Network queried ability of staff with special IT equipment to be able to encrypt documents with a password. No issues identified.
HR	