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

Date: 14/05/2024
Our ref: 01/FOI/24/012093/C

FREEDOM OF INFORMATION REQUEST REFERENCE NO: 01/FOI/24/012093/C

I write in connection with your request for information dated 08/02/2024, received by Greater Manchester Police (GMP) for the following information:

2. Use of Language Policy

3. GMPs Data Download Policy

4. GMPs Reflective Practice Policy

5. Police Officer Suspension Policy / Guidance

6. GMPs Ethical Social Media and Online Communications e-learning training package (March 2023).

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 some of the information you have 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. 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 policy and procedure documents, 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 for those pieces of information.

Please find the rest of your requested information below.

2. GMP does not have a specific "Use of Language" policy. Please see the attached Service Confidence Policy and Procedure which may address your requirements. Additionally, conduct as it relates to language is judged against the Standards of Professional Behaviour defined at schedule 2 of the Police (Conduct) Regulations 2020 for police officer and the Police Staff Council Joint Circular Number 54 (2008) for police staff.

3. Please see the attached Appropriate Use of Information and Technology Procedure.

4. GMP do not have a 'Reflective Practice' policy. The reflective practice review process for police officers is mandated by the Part 6 of the Police (Conduct) Regulations 2020 and the Home Office Statutory Guidance on Professional Standards, Performance and Integrity in Policing. Some further guidance is also available from the Independent Office of Police Conduct.

5. GMP do not have a 'Police Officer Suspension Policy.' Police officers are suspended against the test set down at regulation 11 of the Police (Conduct) Regulations 2020 and having due regard to the Home Office Statutory Guidance on Professional Standards, Performance and Integrity in Policing.

6. This information is not held by Greater Manchester Police. The training package in question belongs to the College of Policing. Please contact them to obtain this information.

Service Confidence

Policy & Procedure

Greater Manchester Police

Oct 2021

POLICY & PROCEDURE IMPLEMENTED: Oct 2021

REVIEW DATE: Oct 2024

POLICY & PROCEDURE OWNER: Head of Professional Standards Branch

APPROVED BY: [redacted]

GOVERNMENT SECURITY CLASSIFICATION: Official

IS THE POLICY & PROCEDURE? ☐ New ☑ Revised

IF REVISED, PLEASE COMPLETE TABLE BELOW

VERSION NO	DATE	SUMMARY OF CHANGES	AUTHOR(S)	PUBLISHED ON CCOs
1.0	Feb 2016	Updates implemented following scheduled review of 2009 Policy.	[redacted]	
1.1	Apr 2016	Amended following consultation		
1.2	May 2016	Amended after COG feedback on 19 Jul 2016. Implemented 18 Aug 2016.		
1.3	Feb 2017	Section 5.1 amended due to outcome of misconduct hearings under legal chairs. Both the Federation & Supts. Association consulted and approved wording.		
1.4	Oct 2021	Supporting legislation updated; name change from Counter Corruption Unit to Anti-Corruption Unit; uploaded to new policy & procedure template.	[redacted]	

Table of Contents

1. Policy Statement

Greater Manchester Police (GMP) recognises that it is legally accountable and subject to public scrutiny in respect of its delivery of policing services. It also acknowledges that in order to maintain and enhance public confidence in the Force it must create an ethically robust, corruption resistant organisation. The Force will take positive action to protect its staff, members of the public and its assets from risk.

1.1 Aims

The main aims of this policy and procedure are to:

a) Provide an ethical framework to address loss of confidence by the Force in any particular individual/s when serious concerns arise as to their suitability to perform a specific role or duty.

b) Protect the integrity of the organisation, individuals and operations

This document is designed to ensure all police officers are fully aware of their respective and joint responsibilities regarding confidence issues and required to behave with integrity as set out in the Code of Ethics. It is underpinned by procedures that detail the steps to be taken at all relevant stages.

The main objectives of this policy and procedure are to:

a) Protect the Force from organised groups or individuals who would benefit in any way from corrupting its staff;

b) Protect all police officers from being subjected to unnecessary or unwarranted pressures, from organised groups or individuals, to compromise their professionalism and integrity;

c) Protect the public from any potential reduction in efficiency of the police service or any increase in non-legitimate activities of any organised groups or individuals;

d) Establish an ethical framework for dealing with those situations where management action is necessary without overt criminal or misconduct proceedings and where the reason for the action is based on information or intelligence that raises serious concerns about a police officer occupying a particular post or carrying out a particular role; and

e) Establish the need to apply fairness, objectivity and proportionality in the application of the procedure.

2. Scope

This policy and procedure applies to all police officers including Special Constables working in GMP.

The Chief Officer lead for Professional Standards is the Deputy Chief Constable (DCC).

3. Roles & Responsibilities

The responsibilities of the various parties involved in the delivery and operation of this policy and procedure are outlined below:

a) There is a responsibility on all members of staff to report any information or intelligence that raises concern over the integrity of any member of staff;

b) The Head of Anti-Corruption Unit (ACU) will be responsible for recommending case conferences, maintaining confidential records in relation to the procedure and keeping an overview of all ongoing cases;

c) The nominated Assistant Chief Constable (ACC) will convene case conferences as required;

d) The relevant Territorial or Branch Commander will attend case conferences, interview individuals concerned, implement training/development and monitoring;

e) The Head of HR Operations/People & Development Branch will attend case conferences;

f) Legal Services will attend case conferences and will ensure compliance with Human Rights and Employment legislation;

g) The DCC will consider the recommendations of case conferences and the outcomes of interviews with individuals concerned; and decide on measures to be implemented;

h) The Chief Constable (CC) will provide the final level of appeal against the decision;

i) The Review Officer, on behalf of the CC, will conduct any appeal against the decision of the DCC;

j) The Monitoring Officer will have responsibility for 'hands on' management of action plans and agreeing time scales for monitoring and review of performance; and for supervision of health and safety and welfare issues. This person will be of the rank of Inspector or at least one rank higher than the individual subject of this procedure, whichever is the higher.

4. Terms and Definitions

4.1 Serious Concerns

It is not possible to provide a precise definition. Each set of circumstances must be judged on merit. As a guide, however, considerations could include:

a) Whether the alleged action(s) of the individual concerned was / were undertaken knowingly or recklessly;
b) A risk assessment of the likelihood and impact of recurrence;

c) The damage to the credibility of the individual as a 'witness of truth' in Police/CPS Prosecutions, and the requirements for disclosure of such issues to prosecutors;
d) The nature of the current role or duties, and an assessment of potential risk to the public, colleagues, investigations or operations if the individual remains in post;
e) An assessment of risk caused by improper association with criminals or their close associates, and the potential for corruption; and
f) Suspected dishonest or unethical conduct, or corruption.

4.2 Confidential or Source Sensitive Information

This will be considered as information or intelligence obtained legitimately but which legislation prohibits use of other than for intelligence purposes, or where disclosure would compromise and put at risk investigations, investigative tactics or individuals.

5. Procedure

5.1 Using this Policy and Procedure

Whenever any member of staff comes into possession of any information or material that raises concerns about the integrity of any member of the Force, they are under a duty to report it (see Section 10 of the Code of Ethics which relates to the standards of professional behavoiur around challenging and reporting improper conduct). Mechanisms for reporting include Crimestoppers, the Integrity Line, internal reporting to managers and direct reporting to the ACU.

The ACU will be responsible for evaluating the information/material and ensuring that it is correctly investigated. It will also test the credibility of the information or intelligence that has been made available. Conventional criminal or disciplinary outcomes will be sought whenever appropriate. However, if at any stage of the investigation it becomes apparent that criminal or misconduct proceedings are not possible or appropriate, or having taken misconduct or criminal proceedings the outcome does not diminish the risk posed by the individual to the public or the organisation, then the ACC will consider the invocation of this Service Confidence Policy and Procedure.

The threshold for invoking this policy and procedure is high and it should only be considered where it is believed that the individual concerned poses a risk to the public, themselves or the organisation.

It must be emphasised that criminal or misconduct procedures will always remain the preferred course of action, and only when they prove to be unsuitable or the outcome does not diminish the risk posed by the individual to the public, themselves or the organisation will this Service Confidence Policy and Procedure be invoked.

Concerns about achieving a balance between the needs of GMP and the rights of the individual should be addressed by:

(a) Adopting an open and transparent system within legal constraints;

(b) Allowing individuals to be represented and the adoption of a reviews process;

(c) Maintaining a clear position that the use of the procedure is about the protection of staff and GMP by management action and not misconduct procedures or sanction.

There will be occasions when verifiable confidential or source-sensitive material comes to the notice of investigators, which brings into question the suitability of a police officer to continue to perform their current role or duties. When the circumstances do not warrant criminal or misconduct proceedings, yet are such as to raise serious concerns that require immediate management action both for the protection of individuals and the Force, individuals will be considered for transfer to a less vulnerable post.

The test of whether there are 'Serious Concerns' about an individual's integrity will be based on an assessment of all the intelligence and evidence, including source sensitive material. The information must establish that, on the balance of probabilities, the individual's integrity is in question. Due regard will be paid to the principles of fairness as outlined above. This test is to be applied at all stages of the procedure.

GMP acknowledges that this procedure may impinge upon aspects of the Human Rights Act 1998, in particular:

- Article 6 - Right to a fair trial
- Article 8 - Respect for private and family life
- Article 11 - Freedom of peaceful assembly and association
- Article 14 - Prohibition of discrimination
- Equality Act 2010

Further legal basis for this procedure is provided by:

- Police (Conduct) Regulations 2020
- Police (Complaints and Misconduct) Regulations 2020
- Police Conduct Regulations 2012 (as amended 2015)
- Schedule 3 to the Police Reform Act 2002
- Investigatory powers Act 2016

The existence of the above articles does not prevent the imposition of lawful formalities, conditions, restrictions or penalties on the exercise of these rights by citizens, including police officers and special constables which may be necessary for a number of reasons, in particular:

- For the prevention of crime or disorder
- For the prevention of the disclosure of information received in confidence
- For the protection of the reputation or rights of others

5.2 Stages

Stage 1 - Referral

Where, following a misconduct/discipline investigation, serious concerns are raised regarding the integrity of an individual in question, the Chair has a duty to make a report to the Head of the ACU.

Where information or intelligence becomes available which raises serious concern that an officer's integrity is in question, the recipient has a duty to make a report to the Head of the ACU.

The Head of the ACU will make a risk assessment based on all the material, including source sensitive material, and will, when appropriate, recommend that a case conference be called.

In so doing, the Head of Professional Standards Branch (PSB) will consider the criteria set out in Stage 2, paragraph 2 below, together with any other relevant information. Where the decision is made not to take the matter further, the Head of PSB will record this in the file confidentially and the procedure will be taken no further. Depending on the circumstances – covert or overt investigation – this will be responded to accordingly. Where an officer is aware of the process they will be updated on the conclusion, otherwise they will not be told. The file will be retained for seven years in case of any Civil Law redress.

Where the risk assessment calls for a case conference, the Head of PSB will forward the papers to an ACC. The ACC will then further review the matter and will decide whether a case conference ought to be convened. Where the decision is taken to proceed to a case conference it shall be held as soon as is reasonably practicable with the ACC sitting as the Chair.

Stage 2 – Case Conference

If the nominated ACC supports the recommendations, as above, they will call a meeting which will involve, as appropriate, all or some of the following:

(a) The nominated ACC
(b) The Territorial or Branch Commander of the individual concerned or their nominated deputy
(c) The Head of ACU
(d) The Head of PSB
(e) The Head of HR Operations
(f) A senior member of Legal Services
(g) The Force Operational Security Advisor (OPSY)
(h) The Police Federation, on invitation
(i) Any other personnel that the ACC believes can give material assistance

During the case conference the matters to be addressed will include Human Rights considerations, in particular article 8 of The European Convention on Human Rights and the Equality Act 2010. The following questions should be considered;

(a) Is the proposed course of action necessary and if so why?
(b) Is there a legitimate aim and if so what is it?
(c) Is the course of action to be taken proportionate to the intended aim?
(d) Is there a less intrusive but equally effective alternative course of action? If so has it been considered and what was the outcome?
(e) What is the likely impact upon the individual concerned and is this proportionate with the proposed course of action?

The meeting will be closed and confidential with the aim of a free and frank exchange of information and intelligence about the individual. Everyone invited will be expected to sign a confidentiality agreement (Appendix A). This meeting will decide whether to carry on with the policy and procedure and, if so, to consider and recommend:

a) What can be discussed beyond the closed meeting; (nothing will be disclosed which would frustrate any criminal or misconduct investigation, or the prevention or detection of crime; damage national security; breach any statute; compromise or endanger any operation or individual).

b) The detail of what protection measures should be put into place to monitor the individual and protect the organisation. To provide advice if appropriate to the individual to prevent further breaches.

c) If there are any vetting implications that should be brought to the attention of the Force Vetting Officer.

d) What can and cannot be disclosed to the individual and/or his or her representative.

e) Whether the matter needs to be referred to next stage i.e. to the DCC.

Minutes will be kept of the conference and a full record of the decision-making processes maintained and kept on confidential file within the ACU.

Where the case conference agrees that action needs to be taken, the matter will be referred to the DCC who will add their recommendations.

Stage 3 – Informing the Individual

The Territorial or Branch Commander will then meet with the individual concerned to inform them of that referral. In accordance with normal practice, the individual will have the right to be accompanied at that meeting by a friend or a member of a Staff Association. Minutes will be maintained of the meeting and retained with the confidential file at the ACU Intelligence Cell. The meeting will address:

a) The purpose of the meeting and the procedure being followed

b) The recommended action plan, redeployment or other intervention for the individual (this may need to be implemented with immediate effect prior to any appeal being considered)

c) The individual's right to make a written submission to the DCC within 14 days of the meeting with the Territorial/Branch Commander

Wherever possible the individual will be informed of the reasons for the recommended action plan, redeployment or other intervention. However, nothing will be disclosed which might:

a) Impede the apprehension or prosecution of offenders;
b) Frustrate any investigation, or the prevention and detection of crime;
c) Damage national security;
d) Breach any legislation;
e) Compromise or endanger any operation or individual.

When disclosure is not appropriate, the individual will be told that the action recommended is being effected on the basis of source sensitive information for the operational needs of GMP and that further disclosure is not appropriate at the present time for those reasons above.

Stage 4 – Decision Making Process

On receipt of a referral from a case conference, following the 14 days allowed for an appeal (in exceptional circumstances the review may take place immediately), the DCC shall consider:

a) Whether there is sufficient evidence to support the recommendation
b) Any submission provided by the individual. (If none is available or the individual requests more time to prepare, this will not preclude the DCC from making a decision to implement the procedure and recommendations forthwith)
c) Whether the action plan, redeployment or other intervention recommended is necessary, proportionate and non-discriminatory, taking into consideration the Equalities Act 2010

The DCC will, within 21 days, decide whether to implement the recommendations and maintain a record of this decision, which will form part of the confidential file held at ACU.

In all cases, the individual will subsequently be notified by the Territorial/Branch Commander of the DCC's decision.

5.3 Appeal Process

An individual can appeal against a decision made under the policy and procedure. The application must be in writing and made to the CC within 14 days of the individual being informed of the decision of the DCC. The application must give the reasons and grounds for the appeal request.

The CC will review the decision taking into account the material in the application.

The review process will:

a) Test the integrity of the process
b) Test the strength and quality of the information and or intelligence on which the decision was based
c) Ensure that the decision is proportionate, necessary and non-discriminatory
d) Consider other options, if appropriate

The review process will be completed as soon as practicable and within 20 working days. The Territorial or Branch Commander will notify the individual of the result in person.

All reasonable steps should be taken to resolve appeals and the individual will be notified of the result within 21 days. The CC should consider whether the decision to invoke the Service Confidence Policy and Procedure was necessary, proportionate and non-discriminatory.

The decision of the CC will be final.

The GMP grievance procedure cannot be used to appeal against decisions made under this policy and procedure.

5.4 Records and Briefings

The Head of ACU will retain supporting documentation and other material at each stage of the implementation of this policy and procedure.

If the decision involves transfer to a different area of command, the Head of the ACU will be responsible for ensuring that the receiving Territorial Commander or Branch Head receives an appropriate briefing. A briefing paper will form part of the individual's personal file.

5.5 Monitoring

The relevant Territorial or Branch Commander will be responsible for any training or development issues resulting from use of this policy and procedure and will create an appropriate action plan for the individual aiming to regain the confidence of the organisation. Any welfare issues that may arise from the process must also be considered.

If there are any prohibitions on an individual's operational capacity, for example, not to work on certain issues, access certain material or handle covert human intelligence sources, then the Territorial or Branch Commander will ensure that the necessary procedures are in place to ensure that, should the Territorial or Branch Commander be replaced, the procedure has resilience and the individual is not left unmonitored.

If the individual is subsequently redeployed or transferred to another place of duty, the Territorial or Branch Commander will ensure that any restrictions on the individual are clearly identified to the new Territorial or Branch Commander by confidential correspondence. A copy of this document should be forwarded to the ACU for retention.

Details of any outstanding prosecutions for which the individual has provided a statement of evidence will be obtained by the Territorial or Branch Commander and reviewed by the Head of the ACU who will consider disclosure to the Crown Prosecution Service (CPS) Unit Head or Special Casework lawyer, in accordance with Chapter 18 CPS Disclosure Manual 2005. In cases where the revelation to the CPS is deemed necessary, the individual will be provided with a form of words agreed by the Head of the ACU and the CPS for inclusion on the form MG 6b. This obligation will be effective until the individual has been informed that it is no longer necessary.

Individuals subject to the policy and procedure will be the subject of ongoing monitoring by a supervisor (Monitoring Officer) nominated by the Territorial or Branch Commander and assisted as appropriate by the ACU. Progress against the action plan should be reviewed at least every 12 months. Any further development needs should be identified and addressed.

If the Monitoring Officer believes the action plan has been successfully completed, then the Territorial or Branch Commander should notify the Head of the ACU in writing. On receipt of the notification, the Head of the ACU will present the case papers, together with any further relevant information and intelligence, to the ACC who will reconvene the case conference to consider:

a) Whether the risk of recurrence has reduced sufficiently;
b) The basis of the original decision and its ongoing validity;
c) The potential risk to colleagues, the public, or police operations should the Service Confidence procedure be terminated;
d) Alternative options as appropriate;
e) Issues surrounding any requirement to disclose the process to the Crown Prosecution Service.

The case conference will again notify the DCC of the recommendations and the individual will be personally informed of the decision of the DCC.

If the decision is to terminate the procedure, then the Territorial or Branch Commander should arrange for a review of the individual’s position taking into account:

a) Any learning needs of the individual as a result of being absent from the normal place of duty or identified as a consequence of the procedure

b) Consideration of issues surrounding:
   - Any organisational needs
   - The protection of the individual and all staff
   - Any human rights issues or any other relevant factor

The individual concerned will remain in the post to which they were transferred under the Service Confidence Policy and Procedure. Subject to the issues within the managerial review, consideration can be given to returning the officer to the same, or a similar, role or duties that the officer was performing prior to the Service Confidence Policy and Procedure being invoked if there is a vacancy and the officer wishes for this to happen.

Consultation will take place with the officer subject of reinstatement, and a Staff Association representative, if required. Any disagreements will be referred to the DCC for decision.

Where the Service Confidence Policy and Procedure was implemented covertly, no discussion will take place with the officer but their personal record will be amended to ensure they have the facility to move freely throughout the force.

The briefing paper relating to the individual will be retained within the ACU for the period of seven years but will be removed from the personal file after a period of 18 months following their return to full duties (this timescale is commensurate with the expiration of final written warnings in Home office guidance). The ACU will be responsible for the removal of the briefing document .

The file containing all of the written records for the procedure will be stored by the ACU for a period of seven years beyond a return to full operational duties.

5.6 Scrutiny

All Service Confidence cases will be subject to monitoring and scrutiny by the professional standards governance process.

5.7 Subject Access

Any subject access requests will be managed as per Force policy for subject access.

6. Associated Documents

Code of Ethics

Reporting Concerns Policy and Procedure

7. Statutory Compliance & Consultation

7.1 Statutory Compliance

7.1.1 Equality Act (2010)

In the application of this policy and procedure, Greater Manchester Police will not discriminate against any person on any grounds including the nine protected characteristics, as defined in the Equality Duty, Section 149, and in addition politics, opinion, property, other any other status, defined in the Human Rights Act 1998, Article 14.

This policy and procedure has been written to protect the organisation from risk and to protect individuals, identified as vulnerable to corruption, from people and organisations who may attempt to corrupt them.

This document has been considered in the context of the General Equality Duty. The requirement for integrity in individuals employed by GMP applies equally to all officers, whether or not they share protected characteristics.

Monitoring information will be collected under this policy. We recognise there is potential for disproportionality particularly in relation to ethnicity. To mitigate against this the DCC, in their review of the panel decision, will consider the requirements of the Equality Act 2010.

7.1.2 The General Data Protection Regulation (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 Data Protection Act 1998, particularly relating to their access to, and dissemination of, a wide variety of personal information and intelligence.

This document has been considered in the context of the General Equality Duty.

7.1.3 Freedom of Information Act (2000)

The policy is disclosable under the Freedom of Information Act.

7.2 Consultation

Department	Comments
Police Federation	Consulted and input to the document v1
Superintendents Association	Consulted and input to the document v1
Unison	Consulted v1
Human Resources	Consulted v1. [redacted], Director of People & Development Branch, consulted v1.4.
Training	Consulted v1
Legal Services	Consulted and provided support in production of the document v1 and v1.4

Neighbourhoods, Confidence & Equality Team	Consulted and provided support in production of the document v1
Information Compliance Unit	Consulted and provided input to the document v1

8. Appendices

Appendix A

Confidentiality Agreement

(For Service Confidence Policy Case Conference)

NAME (OF THE PERSON CONCERNED):

DATE & TIME:

Information discussed within this case conference or contained within any documents relating to or used at this conference is to be held in the strictest of confidence and must not be divulged to any other parties except in accordance with any action or request arising from the case conference.

PRESENT: (Print Name & Signature)

CHAIR:

HEAD OF THE PSB:

TERRITORIAL/DEPARTMENTAL COMMANDER:

HEAD OF THE ANTI CORRUPTION UNIT:

HEAD OF HUMAN RESOURCES:

SENIOR REPRESENTATIVE OF LEGAL SERVICES:

FORCE OPSY:

OTHER: (Specify Role, Print Name & Signature)

1.
2.
3.
4.
5.

This Confidentiality Agreement is to be retained with the Case Conference papers by The Head of The ACU

Appropriate Use of Information and Technology

Procedure

Greater Manchester Police

January 2023

PROCEDURE IMPLEMENTED: January 2023

REVIEW DATE: January 2024

PROCEDURE OWNER: Information Security and Risk Management Lead

APPROVED BY: Chief Officer Group, SIRO and Information Assurance Board (IAB)

GOVERNMENT SECURITY CLASSIFICATION: Official

IS THE PROCEDURE: ☐ New ☑ Revised

VERSION	DATE	SUMMARY OF CHANGES	AUTHOR(S)	PUBLISHED ON CCOs
1.0	20-02-07	IT Systems Legitimate Usage Policy published	[redacted]	
1.1	10-08-11	Reviewed and updated to reflect changes to title and associated references	[redacted]	
1.2	14-08-11	Minor amendments	[redacted]	
1.3	29-11-11	Updated to reflect new procedure template	[redacted]	
1.4	14-02-12	Updated following CCU review	[redacted]	
1.5	27-02-12	Minor amendments	[redacted]	
1.6	11-04-12	Minor amendments following 3ami introduction	[redacted]	
2.0	27-06-12	Approved by COG	[redacted]	23 July 2012 (CCO 2012/29)
2.1	14-08-13	Reviewed, updated, plus minor amendments	[redacted]	
2.2	06-02-14	Transferred to updated Procedure Template	[redacted]	
2.3	12-03-14	Transferred relevant CCOs into body of document	[redacted]	
2.4	25-03-14	Updated Appendices with USB and iPad Documentation	[redacted]	
3.0	13-10-14	Minor amends prior to publication on CCO's	[redacted]	13 Oct 2014 (CCO 2014/41)
4.0	19/07/22	Major review/update to: reflect new technologies; shorten the name from 'Appropriate Use of Electronic Communications and Information Systems' Procedure; and incorporate changes requested by Windows 10 team, PSB and Change Programmes (including removal of reference to use of Personal Side of mobile).	[redacted]	

Table of Contents

1. Introduction and Background

This procedure supports the Information Security Policy and aims to protect the confidentiality, integrity, availability and security of information received and stored by GMP, its information technology (IT) systems and all forms of electronic communications.

Communication and information play crucial roles in policing, supporting us in communicating with colleagues, partners, the public and other stakeholders. In order to maintain and protect the reputation of the Force and support operational policing, it is essential that GMP's data and systems are appropriately protected at all times.

Inappropriate use of information and IT systems can compromise the integrity of GMP, jeopardise the prevention and detection of crime and impact on public confidence. It can also result in criminal and/or misconduct proceedings and potential dismissal for the individual concerned.

This procedure makes it clear what is and is not permitted and outlines the responsibilities of staff, line managers and those who monitor information security, integrity, systems and professional standards.

2. Scope

This procedure applies to anyone who accesses the GMP network. This definition includes, but is not limited to:

- Police officers;
- Police staff;
- Contractors working for and on behalf of GMP;
- GMP volunteers;
- Visiting police officers and staff;
- Partners with access to the GMP network;
- Third party suppliers;
- Researchers;
- Work experience students.

For the purpose of this procedure, IT systems include, but are not limited to:

- Workstations, PCs and Laptops;
- Mobile Devices (Blackberry, Android and IOS);
- E-mail and Faxes;
- Transportable media e.g. USB Pen Drives, CDs;
- Telephones (land-line) and Force issued mobiles (non-smartphone);
- Servers and cloud delivered services;
- CCTV images (including body worn cameras);
- Airwave radios.

3. Roles & Responsibilities

It is the responsibility of each individual to deal with information properly and ensure that their use of electronic communications and IT systems is appropriate. Each individual must refer to Chief Constable's Order 2007/35 Item 1 for further clarification on appropriate access to information for policing purposes and inappropriate access to information for non-policing purposes. This Order also contains advice that you must follow in the event that you feel the need to access GMP intelligence systems for personal reasons, to help prevent you and the Force being compromised.

The information processed by Force systems is likely to include personal data which is regulated by the Data Protection Act 2018 and General Data Protection Regulation (GDPR). Unauthorised use or loss of the data is a breach of these regulations and the Force could be issued with a monetary penalty of up to £17.5 million. Deliberately accessing/processing information without authority could be a criminal offence for which the individual would be personally liable. Please refer to the Data Protection Policy for further details regarding compliance with the legislations.

Each individual must ensure that they act in accordance with the standards laid out in this procedure document and all other associated internal and external documents listed in Associated Documents, in a way which maintains the reputation of GMP. Any action that brings professionalism and integrity into question will be dealt with through the appropriate criminal and/or disciplinary processes.

4. Terms and Definitions

Abbreviation/Acronym	Full Name / Description
ACPO	Association of Chief Police Officers.
App Store	Google Play Store or similar.
At Hoc	System that allows trained operators to alert cohorts of staff to specific and relevant information.
BB MDM	Blackberry Mobile Device Management.
BBME	Blackberry Messenger Enterprise.
CCU	Complex Case Unit.
Delegated Authorising Officer	An individual nominated by a Branch Head/District Commander to authorise the provision of USB Memory Sticks on their behalf, whilst retaining accountability for their Delegated Authorising Officer's decisions.
DPA	Data Protection Act.
Encrypted USB Memory Sticks	As per 'USB Memory Sticks' but require a password to access the data contained on them as the data is encrypted.

FOI Act	Freedom of Information Act.
GDPR	General Data Protection Regulation.
IPA	Investigatory Powers Act 2016
MAS	Monitoring and Auditing Software.
MDM	Mobile Device Management software used by GMP to control certain aspects of the functionality and settings of the mobile devices.
NCA	National Crime Agency (replaced SOCA in 2013).
NPCC	National Police Chiefs' Council (replaced ACPO in 2015).
OPTIK	The suite of GMP policing mobile applications.
Personal Data	As defined by the Data Protection Act 2018 and GDPR, i.e. data that can identify a living individual.
PNC	Police National Computer.
SOCA	Serious Organised Crime Agency.
Unencrypted USB Memory Sticks	As per 'USB Memory Sticks' but do not require a password and the data can be accessed by anyone in possession of the USB Memory Stick as the data is unencrypted.
USB Memory Sticks	A portable data storage and transfer device including pen drives. Another word for the generic term of "flash drives" as well as the exceptional external hard drives which may also be issued where large capacity is required.
Work Space	Knox secured area of the GMP mobile devices, used to hold GMP information. This area is better protected than the Personal space.

5. Procedure

5.1 Principles

To protect the information on our IT systems, we need to maintain the confidentiality, integrity and availability of the information by:

- Protecting personal and sensitive data from unauthorised access and disclosure;
- Safeguarding the accuracy and completeness of information;
- Making information and vital services available to users when required, giving due consideration to GMP policies and procedures.

5.2 Access to GMP infrastructure

GMP staff members have several methods of accessing the GMP network. The operating systems and devices will change over time, but the overarching principles will apply irrespective of the actual device in use, unless the exceptions are stated specifically in this document.

Work-based use of IT systems must take priority over personal use. Staff must consider using electronic or IT systems other than those belonging to GMP for personal purposes as much as possible. Social media networks must only be used for authorised work-related use within working hours. See Appendix A for more information on use of social media.

5.3 Standards Expected

GMP expects all use of electronic communications and IT systems to conform to the highest professional standards, as well as:

- To be accurate, complete and timely;
- To be appropriately secure;
- To be shared only when appropriate;
- To be in accordance with legislative requirements, government guidelines and good practice;
- To avoid behaviour, actions, language or images which could be considered to be discriminatory or offensive to an individual or group of people;
- Only use Force-approved transportable media when absolutely essential.

All staff must:

- Ensure that all information is marked and dealt with in accordance with Government Security Classifications - the GMP network is accredited to OFFICIAL classification but certain applications on the network are operating data of a sensitive nature and are classified as OFFICIAL-SENSITIVE;

- Ensure that all information entered onto GMP and other relevant/approved systems is as accurate and relevant as possible – the quality of information has a direct impact on policing and public confidence;

- Comply with Authorised Professional Practice and the Data Protection Act 2018, Copyright, Designs and Patents and Computer Misuse Acts;

- Ensure that access to information is controlled in accordance with legislative requirements and information is shared only when appropriate to do so in line with data sharing agreements;

- Ensure that information is protected and kept securely, with adequate precautions taken against theft, loss, damage, destruction or misuse of data;

- Ensure that all GMP data is stored in designated centralised corporate repositories, i.e. SharePoint, MS365, One Drive. Data must not be saved on the C:drive or user's personal home drive;

- Ensure that only approved external DVD/CD devices are used when using a GMP device;

- Comply with all policies and procedures for the IT systems they use;

- Report any suspected breaches of information security through their manager or supervisor on Force Form 514B;

- Take particular care with information they are authorised to access, particularly information on any transportable media and information available in printed form; the harm resulting from wrongful disclosure or misuse can be extremely damaging;

- Take necessary steps to ensure, as reasonably possible, that duplication and inaccuracies are avoided when entering information onto IT systems;

- Read and follow all relevant further information contained within the Appendices and action as appropriate.

5.4 Monitoring

GMP has the right to monitor the use of its IT systems and electronic communications. Lawful business monitoring allows a business to monitor, without consent, and to keep records of communications:

- In the interests of national security;
- To prevent or detect crime;
- To investigate or detect unauthorised use of telecommunications systems; or
- To obtain evidence of the communications
    - To establish the existence of fact;
    - To ascertain compliance with practices or procedures; or
    - To ascertain or demonstrate standards such as quality assurance.

In order to meet the requirements set out in the Data Protection Act 2018, and to address the threats highlighted by National Police Chiefs' Council (NPCC) and National Crime Agency (NCA), GMP have chosen to deploy Monitoring and Auditing Software (MAS). This will also allow the System Controller to monitor and keep a record of activity on GMP computer systems for the purpose of preventing and detecting crime. GMP will examine the content of business and personal communications when it is necessary, justified, proportionate and authorised by the Chief Superintendent at Professional Standards Branch (PSB).

Lawful Business Monitoring as a result of intelligence, or as part of a criminal investigation is the responsibility of the PSB, The monitoring will not be speculative or random and any activity will be justified, necessary and proportionate and will follow the same principles and considerations as the Investigatory Powers Act 2016.

In both criminal and misconduct cases, the use of Lawful Business Monitoring will be considered on a case by case basis. The process will be scrutinised by appropriate consent levels being in place, and with authority from a PSB Superintendent.

When using GMP systems and electronic communication, staff must not automatically expect privacy and be aware that the information they communicate may be monitored. Appendix B contains general information about communications that are routinely monitored, personal privacy, E-mails, internet, telephones plus guidance about intrusive monitoring for line managers. It is advised that all staff familiarise themselves with this information.

5.5 Passwords

User identity numbers (PINs) and passwords are the main method of authenticating staff onto GMP systems. Your password identifies you and staff must not reveal their password to anyone else. There must be no occasions when staff members have to use someone else's PIN/User ID and password to carry out their duties. Staff will be held responsible for any activity conducted under their own account. If you believe there are circumstances which require you to divulge your password to a third party, you must contact the Information Security Manager for advice on #ISBSecurity before doing so. Appendix C contains advice on selecting passwords, changing password and guidance for line managers to ensure correct levels of access for staff.

5.6 Use of GMP Electronic Mail (E-mail)

Staff members are expected to manage their E-mail accounts regularly by deleting any E-mails no longer needed for GMP business. The retention period for information will be dependent on the purpose for which it is held. Information must be retained and disposed of in accordance with the Force's Retention and Disposal Schedule. All unwanted E-mails over 90 days old are to be deleted from mailboxes. When using the delete button, E-mails are transferred to the "Trash Folder" or the "Deleted Items Folder". The contents of these folders must also be deleted, thereby complying with the Information Commissioners guidance on the double deletion of E-mails.

E-mails may be subject to disclosure under the Freedom of Information (FOI) Act and the Data Protection Act; as such a request could open up an E-mail trail. It is therefore important to ensure E-mail management is undertaken and that everyone must consider the need to only add to an E-mail if it adds value to the subject. All content must be appropriately and professionally worded and must comply with Force policy. Guidance on how to use E-mail appropriately, effectively and in the corporate style can be found in the 'Making Connections Toolkit'.

5.6.1 Access to an E-mail WITH the account holder's permission

All staff must set up their E-mail accounts and nominate their line manager to have access to the E-mails in order to deal with any correspondence in the event of unplanned absence. If you know that you will be absent for some time and wish for others to have access to your E-mails, you must amend the Access Control List (ACL) on your account or use the 'delegation profile' to allow named individuals the access to your account. More information on how to do this can be found on the

"How Do I" intranet help pages. If a member of staff is absent and has not set up an "out of office" response, their line manager must open their E-mail account and set up the response as well as deal with any outstanding correspondence in the person's inbox where appropriate. Management access must not extend to a mail sub-folder named "Unison" for people serving as Unison representatives.

5.6.2 Access to an E-mail WITHOUT the account holder's permission

There may be circumstances in which someone else, usually a member of staff's own line manager, or another manager, can legitimately open their GMP E-mail account, e.g. when the account holder is ill or on extended leave. This is known as third party access. This could also include access to the 'personal' area of the network, known as the 'Y' drive or PIN data area. Such access requests must be raised via the IT User Hub. Every access request will be assessed by GMP on its own merits before authorising such access. This does not give line managers or others authority to access data indiscriminately. When requesting access, you must be aware that the decision whether to grant or refuse access will depend on:

- The urgency or importance of the work;
- The relevance of the current business need;
- The expected duration of the account holder's absence;
- The availability of other suitable measures, such as asking the sender to send the E-mails to another person.

Management access must not extend to a mail sub-folder named "Unison" for people serving as Unison representatives.

5.6.3 E-mail Calendar

As part of the E-mail account, there is calendar functionality which allows, amongst other functions, calendars to be interrogated for purposes such as booking meetings, etc. The default for the calendar function will be allowed for "all" to view. If there is something in a staff member's calendar that they do not wish everyone to view, they can use the "private" function when they originate the entry. More information on how to do this can be found in the **'**How Do I**'** intranet help pages.

Appendix D contains further information on use of E-mail, sending E-mails outside the European Economic Area and SPAM, Phishing or hoax E-mails. It is advised that all staff familiarise themselves with this information.

5.7 Use of Internet

All staff can access the internet from any workstation. Use of the internet must be commensurate with your duties and must be justifiable. GMP will not tolerate the use of GMP equipment for any inappropriate activity such as downloading offensive documents, text or images. If you are in any doubt about a course of action, take advice from your line manager.

GMP IT and communications systems are provided for use in the course of, or in connection with GMP business only. However, GMP does permit limited and reasonable personal use of GMP telephone, E-mail and access to the internet. It is important that on these occasions access to the systems:

- Is only outside working hours (i.e. in breaks/refreshment breaks or before or after recorded working hours);
- Will not negatively affect the reputation of GMP or public confidence;
- Is in accordance with the guidance and standards laid out in this document.

In addition to the above, legitimate personal usage must be:

- Reasonable in terms of amount of time spent;
- Justifiable in terms of cost (if any) being met from public funds.

5.7.1 Overt use of internet

Staff must be aware that when visiting an internet site from a GMP workstation the site might log the fact that they are located at GMP. Any activity that they engage in may therefore affect GMP. Any staff or teams wishing to covertly access the internet need to be aware of this fact as it may compromise their operations. Further advice on covert access must be obtained from the Force Intelligence Bureau Covert Section.

5.8 Use of GMP Airwave Radios

Airwave is a sophisticated and complex radio system. Although Airwave terminals are encrypted, care must still be taken to avoid the transmission of any information that may be of use to unauthorised persons who may overhear messages. GMP radios are not to be used for:

- Unlawful activities;
- Any other activity which would constitute an act of misconduct.

All users must read GMP's Airwave Policy and Procedures, which provide guidance for good working practices and must be adhered to for the benefit of all users. If any member of staff discovers or suspects that a radio is lost or stolen, they must report the matter immediately to their supervisor, Radio Custodian and subsequently to Radio Network Services (during normal working hours) or the Force Duty Officer (out of hours) who will make immediate arrangements for the radio to be disabled from the system.

5.9 Management, Issue and Audit of USB Memory Sticks

The Force has software which enforces controls on the ability to connect USB memory sticks, and potentially other device types, to GMP desktop and laptop computers. This ensures that unapproved and unauthorised USB memory sticks and other devices cannot be used. It also provides extensive audit capabilities to enable the use of USB devices to be monitored. The USB control software is configured to allow only approved encrypted USB memory sticks to be written to, i.e. staff cannot

freely copy information from GMP systems to a USB memory stick. However, it will allow any device to be read from. This is to facilitate legitimate access to information received on such devices from third parties. The purpose is to protect GMP data from compromise and/or loss. It is not intended to prohibit the legitimate business use of a USB memory stick to view non-GMP data, e.g. CCTV footage from third parties.

5.9.1 Issue and use of Encrypted USB memory sticks

If any officer or member of staff believes that it is necessary to use a USB memory stick to undertake an essential business process, they must obtain an approval from their line manager and submit a request on the IT User Hub. Where the USB memory stick is to be used to transfer data, the line manager must be assured that the recipient has a legitimate need to have this information. This legitimate need will be detailed in the appropriate Information Sharing Policy. The relevant Branch Head/District Commander or Delegated Authorising Officer must ensure there is an essential business need for the use of a USB memory stick and the overarching consideration in permitting the use of a USB memory stick must be the protection of GMP information; therefore, any risk posed by the potential loss of the USB memory stick needs to be mitigated. USB memory sticks must not be routinely issued on a permanent basis.

The officer or member of staff who requires the USB memory stick must complete and sign the Agreement document at Appendix E and submit it to their Branch Head or District Commander or Delegated Authorising Officer. Once the USB memory stick is received, the recipient must submit an IT User Hub request to enable it to connect to a GMP device. The recipient must then update the owner information fields on the USB memory stick encryption software when setting their password for the first time. At the end of the authorised period the person allocated the USB memory stick must delete all data from the memory stick, including their owner information, and arrange to personally return it to IS Branch.

5.9.2 Issue and use of Unencrypted USB memory sticks

The USB control software will prevent information being written to unencrypted USB memory sticks. It will allow any device to be read from which will facilitate legitimate access to information received on such devices from third parties. The issuing of an unencrypted USB memory stick will only be approved in **very exceptional circumstances**, e.g. where there is no capability to interact with the USB memory stick to enter the passwords. The risk to the Force and the individuals concerned is raised significantly when unencrypted USB memory sticks are used. The process for issuing unencrypted USB memory sticks is the same as described in Section 5.9.1. The recipient must be aware of Data Protection Act 2018 and GDPR compliance. At the end of the authorised period the person allocated the USB memory stick must delete all data from the memory stick, including their owner information, and arrange to personally return it to IS Branch.

5.9.3 Use of USB memory sticks to view non-GMP data

Where information is presented to GMP on a USB memory stick which needs to be assessed as possible potential evidence, then normal evidential processes will apply and NPCC Guidelines in respect of Digital Evidence must be adhered to. Where non-evidential information is presented to GMP on a USB memory stick which needs to be assessed, e.g. training material, then these USB memory sticks can only be viewed on GMP computer. Once viewing has been completed it may be appropriate to save the information. The USB management software supports this process by enabling such USB memory sticks to be read from but not written to.

5.9.4 Loss of USB memory sticks

In the event of any USB memory stick being lost by a member of staff; their line manager must be notified as soon as possible. Force Form 514B must be completed by the person reporting the loss. This will ensure that the correct process for data breaches/losses is followed.

5.9.5 Audit

Auditing these procedures will be incorporated within the Force Audit Plan. The Force USB Memory Stick Issue Log with details of USB recipients is subject to review and will also be made available to audit personnel on request. Staff issued with GMP memory sticks must make them available and accessible to audit personnel on request.

5.10 Management, Issue and Use of GMP Mobile Devices

This procedure documents the current approach to Force-issued mobile devices and covers their authorisation, issue, usage and return. This document will be updated as GMP device usage and/or the security threats change, therefore GMP mobile device users must ensure they keep themselves updated with the changes. Where the conditions and principles within this document are not complied with, the right of personal use will be withdrawn and the misuse or abuse may result in action under the disciplinary procedure being instigated.

5.10.1 Issue of GMP Mobile Devices

If an officer or member of staff believes that it is necessary to use a mobile device to undertake an essential business process, they must obtain the appropriate approval from their line manager and submit a request on IT User Hub. The overarching consideration in permitting the use of a mobile device must be the protection of GMP information and therefore the user must ensure that any risk posed by the potential loss of the mobile device is mitigated. Any breach of contents of this section may lead to action under GMP's disciplinary procedure and/or result in the commission of criminal offences.

5.10.2 Use of GMP Mobile Devices

5.10.2.1 General Use

The device must be used with SIM Cards issued by GMP. SIM swapping is not permitted. Voicemail messages must be appropriate and professional.

5.10.2.2 Data usage

Staff may make reasonable personal use of the internet but it must not be used for streaming video or films unless connected to Wi-Fi. Additionally, devices must not be used as Wi-Fi hotspots. GMP's current carrier contract provides an amount of data to be pooled across the Force. This will cover all work needs and a small amount of personal usage. Therefore, whilst GMP permits staff to make use of the data allowance for personal use; staff must not use data-hungry applications over GMP data. If an individual is using significant amounts of data, their manager will be asked to confirm that the usage is for policing business. Any personal use that incurs additional cost to the Force may need to be reimbursed.

5.10.2.3 Overseas use

All devices are configured to function outside the UK; however, may require additional approvals from your line managers before such use can be conducted. For mobile phones, overseas data usage will incur costs to GMP which will be presented to the user along with any call and text costs. The user will be required to identify usage outside legitimate GMP use and reimburse the Force.

Appendix F contains further information and advice on overseas use and use of wireless networks. Staff with a GMP device must familiarise themselves with this guidance.

5.10.2.4 Use in public areas

The mobile devices are intended for use outside of the confines of a GMP office. Users must therefore take appropriate steps to ensure GMP data remains secure whilst the device is in use. Users must be aware not only of the people around them in the immediate vicinity, but also of the wider environment. Cameras can be used to capture images of screens in plain sight; hence GMP mobile devices could easily be targeted. It may be appropriate for the user to relocate or reposition the device to ensure privacy. The use of Bluetooth must be consistent with the guidance in this policy.

5.10.3 Mobile Device Management

5.10.3.1 Device Lock

Android devices are secured with the device lock set. This will ensure that if the device is stolen, five minutes after it was last used the device will be password protected. GMP data held within the workspace is protected by the workspace password five minutes after the workspace was last used. All devices can be remotely wiped and sit behind 2-Factor Authentication (RSA token). It is important to note that pressing the power switch locks the device.

5.10.3.2 Workspace and Device Wipe

The Workspace Wipe is initiated by the Android OS, when the work space password is input incorrectly more than five times. The workspace wipe will remove all GMP data from the Android device, but will not disable other functionality.

The device wipe function will be initiated by the Android OS, when the device password is input incorrectly more than 10 times. The Device Wipe will remove all GMP and user data from the device, returning it to the factory-issued condition. Once complete, the SIM card within the device continues to function.

Users must be aware that exceeding the password limits will result in all unsaved GMP data being lost. Users are therefore advised to contact the service desk when they are unsure of their password before they exceed the password limit.

5.10.3.3 Remote Wipe

When a user reports that a device is or may have been lost or stolen, or suspected to have been jailbroken or tampered with, the user must report this immediately. They must report this in the normal manner, by calling 61400, during office hours or the Duty Officer (out of hours) on 66321. The device's internet connection will be used to issue the wipe command, which will result in all user data being securely deleted from the device.

If the device is confirmed as lost or stolen, it is important that the provider is contacted to block the SIM card. This is to avoid any attempts to defeat or avoid the wipe command which can be done by powering the device off and removing the SIM card. Once the Remote Wipe has been performed, the SIM card will continue to function, and thus if the device has been lost or stolen, anyone could continue to incur expenses to GMP through use of the SIM card, unless this has been protected by a PIN.

5.10.3.4 Android OS upgrades

Android devices provide version upgrades to their operating system on a regular schedule. The Information Security Team monitors OS upgrades and appropriate advice will be issued to the users if an upgrade is made available for the devices.

Occasionally, the Blackberry MDM software will be used to reject access to the workspace environment if a specific Android OS upgrade has not been completed. Under most circumstances, users will be given at least one week's notice of such an upgrade enforcement decision.

5.11 Use of GMP Telephones and Faxes

GMP provides fixed telephones and fax facilities for use by its staff in the course of, or in connection with, GMP business. GMP recognises that it is sometimes necessary for staff to deal with personal or welfare issues during the working day and as such will allow limited personal use from GMP fixed phones. This must be notified to the line manager at the first available opportunity. GMP telephone and faxes are not to be used for:

- Unlawful activities;
- Personal financial gain;
- Commercial purposes;
- Any other activity that would constitute an act of misconduct.

GMP will need to be reimbursed any additional cost incurred as a result of personal use of telephones and faxes.

6. Associated Documents

Airwave Policies and Procedures
Authorised Professional Practice
Code of Practice on the Management of Police Information (MoPI)
Computer Misuse Act 1990
Copyright, Designs and Patents Act 1988
Data Protection Act 2018 and General Data Protection Regulation (GDPR)
Data Protection Policy
Equality Act 2010
Freedom of Information Act 2000
Government Security Classifications (GSC) Policy and Procedure
Human Rights Act 1998
Information Security Policy
Lawful Business Monitoring Policy
Making Connections Toolkit, Corporate Communications Branch
Media and Social Media Communications Policy and Procedure
Microsoft Teams Recording Policy and Procedure
Investigatory Powers Act (IPA) 2016
Retention and Disposal Policy

7. Statutory Compliance & Consultation

7.1 Statutory Compliance

7.1.1 Equality Act (2010)

The procedures set out in this document have been considered in the context of the General Equality Duty. The requirement for the appropriate use of GMP electronic communications and information systems applies equally to all staff, whether or not they share protected characteristics.

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

The use of information systems for processing personal or sensitive personal data is governed by the Data Protection Act 2018. The integrity of information stored in GMP systems is dependent on staff therefore all staff members must know their responsibilities in safeguarding the data to ensure the use of information systems comply with the Act.

7.1.3 Freedom of Information Act (2000)

The FOI Act 2000 grants a general right of access to all types of recorded information held by public authorities. Any requests for the disclosure of this procedure must be directed through the Information Compliance and Records Management Unit via the FOI mailbox. They will liaise with the policy owner prior to the disclosure of information contained in this procedure.

For advice and assistance on FOI, contact [redacted].

7.2 Consultation

Department	Comments
ICRMU	Consulted Apr 2022. Amends actioned.
Professional Standards	Consulted 2022 – [redacted], amends made to various sections in respect of Lawful Business Monitoring.
GMP Federation	Consulted Nov 2022. Queries raised but no amends required.
Legal Services	Consulted Nov 2022.
Unison	Consulted 2021 and Nov 2022. Many amends requested and actioned.

HR Branch	Consulted Nov 2022
Staff Associations	Consulted 2021 (amends requested and actioned) and Nov 2022
Staff Support Networks	Consulted Nov 2022

8. Appendices

Appendix A: Social Networking Sites
Introduction, security and personal risks, unacceptable content

Appendix B: Monitoring
Introduction, personal privacy, E-mails, Internet, Telephones, Advice for Line Managers

Appendix C: Passwords
Selecting your password, Changing your password, Advice for Line Managers

Appendix D: Use of GMP Electronic Mail (E-mail)
Use of email, Sending emails outside European Economic Area, SPAM and hoax email

Appendix E: Management, Issue and Audit of USB Memory Sticks
Agreement Form

Appendix F: Use of GMP Mobile Devices
Overseas use, Use of wireless networks, form of agreement

Appendix A: Social Networking Sites

Social networks are online services or sites that are focused on building networks or relationships with people online, either professional or social. Social networking sites allow people to share ideas, activities and interests with other people on the network, and engage in conversations about topics of interest to them. Social networking sites include, but are not limited to, Facebook, Twitter, YouTube, Flickr, MySpace, Bebo, Uniformdating and Friendster. Personal cloud hosting sites are sites such as GoDaddy.com or Wordpress that enable the creation of websites or blogs.

If challenged, staff must be able to justify their use of GMP equipment and systems. Any conduct that breaches criminal law or GMP's Information Security Policy will be dealt with accordingly.

Security and Personal Risks

GMP respects an employee's right to a private life. However, GMP must also ensure that confidentiality, integrity and its reputation is protected. Social networking sites have varying levels of security and as public sites; all are vulnerable to unauthorised access attempts. GMP business is not to be discussed or referred to on social networking sites or other personal cloud hosted services, for example online educational and training services. It therefore requires police officers and staff to:

- Ensure they do not conduct themselves in a way that it is detrimental to GMP;
- Take care not to allow interactions on these websites to damage GMP's reputation, working relationships between colleagues, members of the public or other organisations;
- Not upload any data from GMP's systems, for example, CCTV footage;
- Consider if it is appropriate to identify them as working for GMP.

All police officers and staff have a responsibility to consider the impact of their actions in and outside work that may impact upon GMP's reputation, values and their own position. Anyone who knowingly or inadvertently declare a connection with GMP as their employer or otherwise need to be aware of the personal and corporate risks before making an informed decision on their social networking activity. This includes private messages between site members who may be authorised to access your information. The only occasions where GMP business can be discussed on these sites is when it has been authorised through the Force's Media and Social Media Communications Policy and Procedure.

Police officers and staff must be aware that social networking websites are a public forum and must not assume that entries on any website will remain private. It is advised that you must use the appropriate privacy settings to ensure your profile is protected and not open to the general public. However, the terms and conditions on sites usually include waiving copyright; therefore anything you post could be used by the media or other parties. Local and national media monitor social networks and will be looking for potential stories about GMP and its staff. Identifying that you work for GMP or have a connection to it may put you at risk for being targeted, blackmailed or personal

threats to yourself and your family. You must be mindful of this whilst using such websites personally and maintain the highest professional standards at all times, e.g. references through friendships, updates or photographs which may unwittingly put GMP staff at risk or bring the Force into disrepute.

Unacceptable Content

Any inappropriate comments or images found on social networking sites will be investigated in accordance with Professional Standards of Behaviour for Police Officers, or Police Staff Standards of Professional Behaviour, which if proven may result in dismissal. The investigation will consider whether the allegations bring GMP into disrepute by being one or more of the following examples:

- Abuse regarding religion or religious beliefs
- Defamatory
- Indecent
- Obscene
- Racist
- Sexist and Homophobic

The list presented is not exhaustive.

Police regulations mandate that staff and officers must not compromise their position within GMP with their political or religious views but must maintain their impartiality and integrity. They are not to discriminate unlawfully or unfairly in line with current legislations. An officer's or staff's political beliefs must in no way compromise or affect their duties to the public or their decision making.

Appendix B: Monitoring

GMP uses a wide range of products to gather information for monitoring and auditing the use of systems within the GMP network. Some communications are routinely monitored full time (for example, radio and telephone conversations in Operational Control Rooms) whilst others will be monitored when justified in accordance with this procedure. The methods of monitoring and auditing range from embedded tools in application to those specifically designed for auditing access. Examples of these are:

- Event logs in windows applications;
- Reason code in PNC;
- Monitoring and Auditing Software;
- Digital Voice Recording.
- OPTIK Auditing.

An audit/monitoring tool is deployed on all GMP computers and will capture all actions on that computer. The information will be stored and used with the authority of a Superintendent from the Professional Standards Branch, but only when it is deemed necessary, justified and proportionate to lawful business monitoring purposes, (e.g. in the event of an investigation into suspected misuse of GMP information). See Lawful business monitoring policy.

Personal Privacy

This procedure is intended to take into account legislation that aims to ensure a minimum level of personal privacy for employees in their employment. The Telecommunications Data Protection Directive requires European Union members to protect the confidentiality of communications made over a public telecommunications system. The Investigatory Powers Act (IPA) 2016 fulfils the UK's obligation by making regulations to govern interception and protect confidentiality.

The directive extends to:

- all types of communication made by means of the public telecommunications network, including E-mails and faxes; and
- private networks connected to the public system, such as that run by GMP.

The law prohibits listening to, tapping and storage of communications without consent except where legally authorised. The IPA also created regulations for lawful business monitoring that allow a business to monitor without consent and to keep records of communications for specific purposes.

E-mails

All E-mails received by or transmitted by GMP are routinely recorded and captured by MAS. Staff must be aware that MAS cannot differentiate between personal and business E-mails and personal E-mails cannot be afforded any degree of privacy. Details are recorded for the sender, intended recipients, subject and content.

Internet

All internet access and activity is monitored and logged by GMP, with the PIN/User ID being used as the source for recording these details. All sites browsed or visited by staff are also recorded. The Information Security Team produces monthly reports and if any misuse is suspected or detected, this is forwarded to Branch/District contacts for further investigation.

Telephones including Mobile Phones

The Information Services Branch records details of all telephone calls made from GMP extensions and bills are sent to Branch/District contacts for checking any misuse. All telecommunications using GMP lines are subject to monitoring in accordance with Lawful Business Monitoring and IPA.

GMP will monitor applications and activities of GMP mobile phones. All transactions will be communicated over the Mobile Device Management (MDM) infrastructure and all activities on the OPTIK application will be stored and be auditable. Use of OPTIK must not occur whilst not on duty. Overall usage including calls and data will be monitored to ensure GMP does not incur costs for excessive use.

If Blackberry Messenger (BBME) is installed on a GMP device, GMP will record the application installation and the respective device, e.g. Samsung S9. All data transmitted over this solution is stored and controlled within GMP servers and is fully auditable. All messages must comply with principles outlined within this document.

GMP uses a Force wide communications platform called AtHoc. This system allows trained operators to alert cohorts of staff to specific relevant information via E-mail, SMS, App, BBME or Text to Voice. Recipients can then respond to alerts by choosing the relevant pre-defined response options. This system is fully auditable for all transactions and records time/date stamps of when alerts were created, how they was sent and to whom, and any responses. Users can install the app to their work device and on their personal device if they wish. The app does not provide GMP with any other information from the device. The use of At Hoc Alerts is primarily for Force wide and partner emergency agency communications in times of major incidents. The system is not to be used for non-GMP information.

Advice for Line managers

The approval of the Professional Standards Branch Superintendent, is required for monitoring. Examples of where this could be used are where confirmation that individual member of staff has been abusing the E-mail system and there is a requirement need to discover the amount of E-mails being sent and to whom.

Appendix C: Passwords

Selecting your password

When you are first issued with a password, you must change it at once. Failure to do so will mean that the password will be known to at least one person other than you. It is recommended that the password must consist of:

- At least nine characters;
- Letters and numbers;
- Upper and lowercase letters;
- Include a special character (i.e. a '!' or '.').

To make your password 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”.

You must avoid using words or terms that reflect your lifestyle, such as:

- Names of your spouse, child or pet;
- Car model or registration number;
- Address or telephone number;
- Your rank or post title;
- Any reference to the police or GMP.

The above restrictions may appear to make it difficult to choose a password that you can remember, but there are still many options. E.g. you could base your password on the initial letters of words in a favourite song or poem.

Changing your password

If you have any indication or suspect that your password has been compromised, you must change your password. To change your password you will have to enter your old password and then enter your new password twice. This ensures there are no discrepancies when entering your new password.

Advice for Line Managers

Your staff must not share passwords but must have the correct level of access to be able to carry out their duties when transferring or commencing employment.

Appendix D: Use of GMP E-mail

Use of E-mail

E-mail is the prime vehicle for communication across the Force and must be used in preference to paper transactions wherever possible. Care must be taken when using E-mail as a means of communication as all expressions of fact, intention and opinion via E-mail may bind you and/or GMP and can be produced in court in the same way as oral or written statements. The same principles apply to information exchanged in this way as apply under the terms of your employment contract to any other means of communications. The nature of the information being communicated over GMP E-mail must be considered as some subjects may not be suitable for E-mail, e.g. sensitive personnel information (medical, welfare and in-confidence). E-mail is suitable for documents up to and including the GSC marking of 'OFFICIAL' for internal E-mails or E-mails routed securely via PNN and CJX addresses but not E-mails sent to insecure E-mail accounts e.g. sky.com, hotmail.com and anycompany.co.uk. GSC marking must be applied to E-mail in line with Force policy.

GMP does not tolerate any behaviour, action or language that could be perceived to be discriminatory or offensive to an individual or group. Any action that brings your professionalism and integrity into question will be dealt with through the appropriate disciplinary and possibly criminal processes. If you use E-mail for purposes that are not related to your duties you may be asked to justify your actions.

Sending E-mails outside European Economic Area

The Information Compliance Manager in IS Branch, must be consulted prior to sending an E-mail containing personal data outside the European Economic Area (EEA) as additional safeguards must be followed.

SPAM, Phishing and Hoax E-mail

GMP has systems to prevent spam E-mails reaching your workstation but occasionally there may be one that gets to your mail box. You can either delete the E-mail or forward it to the Spam mail box. This is achieved by typing SPAM in the “To” address box.

Hoax E-mails are those that promise untold rewards or dire consequences if the E-mail is not sent to “everyone in your address book”. The only action you must take on this type of E-mail is to forward it to [redacted]. Under no circumstances must the E-mail be forwarded to anyone outside or inside of GMP. A GMP sender will add to the authenticity of such an E-mail. You must always check the authenticity of the E-mails before you forward. If in doubt, do not click on any links in suspect E-mails.

Appendix E: Management, Issue and Audit of USB Memory Sticks

Form of Agreement – Use of USB Memory Sticks

1. I have been authorised to use a USB memory stick in order to undertake an essential GMP business process.

2. I confirm that I am aware that:

- I must only use the USB memory sticks provided by GMP to connect to a GMP workstation or to record, store or forward any GMP data or information in a way that has been approved;
- I must not use USB memory sticks provided by GMP to hold or process any information other than that required for the approved GMP business purpose;
- All material stored on the USB memory stick must be marked in accordance with the GSC and under no circumstances whatsoever must any material that is GSC marked OFFICIAL or higher be recorded on or stored on the USB memory stick. In the very exceptional circumstances that an unencrypted USB memory stick is to be used, under no circumstances whatsoever must any personal data, as defined by the Data Protection Act 2018, nor any material that is GSC marked OFFICAL-SENSITIVE or higher be recorded on or stored on the USB memory stick without the additional authorisation required from the Information Security Manager;
- Responsibility for the security and safe use of the USB memory stick issued to me is mine;
- If the USB memory stick is unencrypted then when not in use it must be stored in a locked container and must never leave GMP premises without the express permission of the Branch Head/District Commander if it contains GMP data. If the USB leave GMP's environment for authorised data sharing purposes, transporting of it must be via secure method such as hand delivered or tracked postal service. A record will be maintained of the location of the unencrypted USB memory stick;
- Under no circumstances must the USB memory stick be used by or transferred to another member of staff;
- I understand that I must make the USB memory stick available and accessible to Audit personnel on request;
- At the end of the authorisation period it is my responsibility to delete all data from the USB memory stick and to return it to the issuing authority.

3. I understand that any breach of this agreement may lead to action under GMP's disciplinary procedure and/or result in the commission of criminal offences.

Signature ..... Date .....

Print Name ..... PIN ……

Appendix F: Use of GMP Mobile Devices

Overseas use

The user must carefully consider the risks of taking their device overseas. They need to consider how they can maintain physical security, especially if on holiday when the user is likely to be separated from the mobile device for considerably longer periods of time than on a business trip. Physical security provision in a hotel might be inadequate. A hotel room safe or hotel reception secure storage is often not adequate to ensure that your device is not compromised. The user must also consider the country they are visiting, as there might be higher risks associated with entering some countries than others. Whilst passing through customs, the device may be removed and out of sight for a period of time and the device could be compromised upon its return, or simply not returned. Consideration must be given to:

- Leaving the device behind;
- Ensuring that Force data is inaccessible;
- Wiping the device on return, after removing relevant force data captured whilst away, to ensure the device is restored to a known secure state. This is especially relevant if the device has been out of sight at any time.

No data must be transferred outside of the EEA, therefore prior to departure any force data that may have been held on the device must be wiped. If there is an operational need for the data to be taken overseas then the Information Compliance Manager must be consulted.

Use of wireless networks

Wireless networks provide high speed internet access but their use is not without risk. All mobile devices will search for known wireless networks and try to connect to them. The best practice for Wi-Fi is therefore to switch wireless off (via the *Settings* option), unless it is needed. If Wi-Fi is switched on, users must observe what network the device connects to and ensure this makes sense, i.e. that it connects to the network you would expect. Users must consider how much they trust a network before using it, based on their physical location. In cases where users trust the physical security around their location as well as the network (e.g. home network at home or any Force HQ network) then the connection can be trusted. Conversely, a hotel network or a wireless café network, for example, must be much less trusted and users must carefully consider their use of the network in these circumstances. Use of 4G networks may be slower but are more likely to be secure.

Form of Agreement – Use of Mobile Devices

I understand and accept that:

- I may only use Greater Manchester Police's Mobile Devices in accordance with force policy and procedures;
- Any knowledge gained about Greater Manchester Police, collaboration or National systems and any Police data obtained via Greater Manchester Police Mobile Devices is for authorised business purposes only and will not be shared with unauthorised parties;
- I will only carry out changes to Greater Manchester Police Mobile Devices that I am authorised by Greater Manchester Police's managers to undertake;
- The device is a personal issued device and as such the individual is responsibility for its physical security and safe operation (ensuring GMP information is properly protected in terms of confidentiality, integrity and availability) lies with me. I will protect with device and the protected environment with a unique password that is at least 8 characters in length with one alphanumeric character;
- By logging on to the Greater Manchester Police's work area of the Mobile Device, I accept that my actions may be recorded and that I am responsible for any actions undertaken from a Greater Manchester Police Mobile Device issued to me;
- I will only store corporate information in the Protected Environment and must not use it to store important or critical information unless a copy of that data is held elsewhere, other than short periods of 'temporary' storage e.g. making notes or taking photographs, until a backup is performed and information is removed from the device;
- All material accessed or stored on the device within the Protected Environment will be marked in accordance with the GSC scheme. In no circumstances whatsoever must any material that is GSC marked OFFICAL-SENSITIVE or above will be processed or stored on the device;
- If I no longer require the device, I will return it to the IS Branch. Under no circumstances must the device will be used or transferred to another user;
- There must be no attempt to jailbreak or otherwise tamper with the integrity of the device. This includes removal or swapping of the SIM card issued by GMP to operate with that specific device without express authority of CAPITA. If I suspect that a device may have been tampered with, I will report it to the IS service desk.
- I have read and agree to abide by the Greater Manchester Police Mobile Device Security Operating Procedure and accept the conditions documented therein.

Signature ..... Date .....

Print Name ..... PIN ……