# How to use MPS data and technology with confidence[1]

# Frequently Asked Questions

## 1. Why policing data matters?

Data is a critical organisational and operational asset. The technology we use to input, share and manage that data helps us to find out what we need to know are designed to help us do so ethically and legally. However, the onus is on each individual who accesses the data and technology to know how to use it responsibly. This short guide helps you understand your responsibilities to do that in line with the MPS Information Code of Conduct and Use of MPS ICT Systems Policy.

## 2. What is important to know

The data and technology context, both in society and in policing moves rapidly. The New Met for London will rely on how we all make better use of data and technology, we have refreshed our policies and practice advice on how you can do that, remaining up to date with existing legislation.

## 3. Who is affected by the policy?

Basically everyone in the Met including all persons supporting the organisation. Besides police officers, police staff, MSC and volunteers [Met personnel], it includes all third-party contracted staff and suppliers i.e. anyone granted legitimate access to Met and National Policing systems, applications, data and communications. The clear expectation is that all authorised persons must fully comply with the conditions of use regarding access to policing systems, data and communications provided for both operational or support policing purposes.

## 4. What data does the policy relate to?

This policy relates to all data we create, collect and record and includes data given to us by the public. Our data holdings are unique and significant and include different data types such as crime records, intelligence, forensics, biometrics, video, audio, statements and more. Much of this data is either operationally sensitive or includes the sensitive personal data of individuals, so it must be protected and only used for legitimate policing purposes.

## 5. What data systems does the policy relate to?

All Met and national policing ICT systems [e.g. CONNECT, C&C and PNC], applications [e.g. BOX, S' Drive and SharePoint] and devices [including mobile IT devices - laptops, tablets and smartphones], plus other communications devices such as fixed telephony,

[1] **MPS Information Code of Conduct and Use of MPS ICT Systems Policy – v1.0 dated 25 October 2023**

Airwave radio, BWV and In-vehicle mobile data terminals are all in scope and therefore subject to similar conditions of access and use. The Use of MPS ICT Systems Policy provides further details, but basically the described systems and technology are valuable resources provided out of the public purse in order to meet primary policing requirements.

## 6. How can I best protect Met data and data systems?

Every day the Met collects, creates and records thousands of data sets, most of it provided by the public, who entrust us to protect it in order to provide an excellent policing service. Much of that data is highly sensitive, biographical in nature, relates to persons at their most vulnerable. It consequently demands the highest standard of care and due diligence by all Met personnel to ensure it is processed correctly. Not only policing specific legislation like PACE must be met, but also other requirements like the Data Protection Act 2018/ UK GDPR, Investigatory Powers Act 2016 and the Freedom of Information Act 2000. The main message is that taking basic due care to apply accurate, timely and relevant data quality recording from the outset largely protects the confidentiality, integrity and availability (CIA) of data. It also helps meet basic legal requirements to protect data. This can be best achieved by inputting data directly in to core operational and support systems [like CONNECT, C&C, PNC] and other designated data repositories. It means the data can be easily located and linked, so that it is readily available when required for policing purposes. We also need to remember to protect all paper documents that contain sensitive information and/ or where they constitute corporate records that need to be retained/ stored securely either locally or centrally.

## 7. I've been personally issued with a Met device. How do the rules apply?

It's important to understand that personal issue does not mean personally owned. Under no circumstances do you 'own' your Met-issued ICT device [which includes your laptop, tablet, and smartphone], any more than you do an Airwave radio. It is business issued device attributable to you regarding its care, control and use primarily to support your business role. Whether you are a Met or a third party employee, if you have a Met device then it has been allocated to you, it is to be personally taken care of during your service. You must therefore promptly report any lost or stolen devices. Any faulty or end of life devices can also be handed in at one of the Tech Bars dotted around the estate before you can be issued with a replacement. Often such devices can be refurbished/ recycled for the benefit of colleagues, or disposed of securely and in line with waste disposal requirements. Don't leave them, or indeed any unwanted ICT equipment, to languish out of sight in pedestals, cupboards or lockers, as they remain a corporate resource. When your service ends, you and your supervisor must also arrange [as part of the leaver's service process] for the return of all ICT and telephony equipment, along with your ID and other Met property.

**8. How is this impacted by the recent smartphone rollout?**

It's essential that primarily Met-approved business connected devices are used to carry out policing duties, rather than any personal or other unauthorised equipment. The smartphone rollout aims to equip you with the best technology you need to carry out your duties in a fast and secure way without compromising yourself or the organisation. Not only are the phones designed to be In-tune configured and secure, they should be able to synchronise to a user's laptop or tablet to enable easy direct access to their Met accounts. The range of apps is already good and growing, including PNC, CAD Lite and Crime Mapping to enable users to conduct quick searches on the go. Users can also take evidential images on the phone's camera and then upload them directly to Evidence.com, via the AXON Capture app, saving much time, effort and maintaining data security. MS Teams, SMS text and calls enable quick and auditable ways to contact members of their team or the public. Where an officer is on duty and has a job smartphone, they should not need to use a personal device for policing purposes.

**9. When can social media be used for Met policing purposes?**

The use of social media/ instant messaging (SM/ IM) for Met policing duties is supplemental to our existing means of external communications such as Outlook email and telephony [calls and texts] delivered via approved Met platforms. WhatsApp and other approved instant messaging applications can be used to send short messages by way of updates to the public, such as victims and witnesses and to communicate with trusted partners. However, SM/ IM must always be used only for policing purposes and strictly as per the rules/ guidance to be found in the Use of MPS ICT Systems Policy. You must not use any unapproved SM/ IM applications. Use of your private WhatsApp account on your own private mobile device to contact the public is not permitted, except in an emergency situation, which you must be able to justify [e.g. when you are temporarily without a Met means of communication and the matter is urgent]. Our corporate internal communications tools, including Microsoft Teams, Outlook email, Chat, telephony and Box have all been authorised for policing use on Foundation and should be used wherever possible in preference to SM/ IM, such as WhatsApp. All SM/ IM apps use will be subject to conditions of use in line with defined policing purposes both applicable to individuals and to ensure chat groups are subject to control. Basically SM/ IM can be used for legitimate police purposes but will usually only be permitted in the following circumstances:

- **Corporate approval of the app**: Only SM/ IM apps that have been approved corporately by the Mobile Applications Approvals Meeting (MAAM) are cleared for policing purposes use; and
- **Local authorisation & rationale**. Unless you are using an SM/ IM corporate account [set up by DMC Social Media desk], you will usually be limited to the use of WhatsApp for policing purposes. Other SM/ IM approved apps, such as BBME

or Signal, might be authorised locally for specific policing purposes on the authority of a local business unit Superintendent/ Director.

**10. When <u>can</u> I use Met devices / systems for personal reasons?**

The policy now reflects further restrictions on 'personal use' of Met ICT systems. With immediate effect, permitted use for personal reasons whilst at work will be strictly limited to:

- Occasional, non-transactional Internet browsing of mainstream websites;
- Making and the taking of limited telephone calls and texts for essential family and domestic purposes; and
- The sending of Outlook emails under the same circumstances [e.g. sending your payslip/ tax documents/ training certificates to your home email account is acceptable].

The use should be limited in time/ scope; reasonable and not interfere with the individual's policing duties. Furthermore, it should not by the nature and content of the communications constitute a breach of any Met policies, professional standards or bring the Met into disrepute. Please note that if you choose to communicate in this way there can be no expectation of privacy on your part due to the lawful business monitoring and audit deployed on Met systems.

**11. When <u>can't</u> I use Met devices / systems for personal reasons?**

The increased restrictions on personal use of Met ICT provides greater assurance that the technology is primarily provided in order to fulfil policing only purposes. It is in your own interest to conduct your private affairs outside of policing on your own computer or mobile phone. Therefore, as a consequence of these restrictions, you are **no longer permitted** to undertake the following on Met ICT systems and telephony:

- any online banking or shopping transactions
- Prolonged web browsing, web streaming, use of webmail or large downloads when connected to the Met Internet
- Make any private social media or instant messaging use
- Create Word, Excel spreadsheets or use Power Apps for personal purposes

If you currently access your personal social media accounts via Met systems, you should delete these from your Met mobile device immediately. Doing this should prevent your personal data from being exposed under lawful business monitoring (LBM) and will help secure your privacy.

**12. How should I manage my personal, welfare, domestic or business affairs whilst on duty?**

It is expected that MPS personnel will ordinarily use their privately owned IT and mobile devices wherever possible to access the Internet, make phone calls and send texts and

emails in their own time [e.g. at work during mealtimes or other breaks]. Only in extreme or urgent circumstances, or where an individual does not have access to their own device, should they use Met equipment and then solely for the family/ domestic reasons already stated in the answer to FAQ10.

**13. Can I use my own personal phone or IT device for Met policing business?**

No, you should not use your personal device for any policing duties. The IOPC recommends that personal devices should not be used to contact members of the public, so you should not do so except in extremis. Otherwise you must wait to contact the person when you are next at a Met building and/ or you have access to Met telephony or a Met device. If for example, you come across an incident off-duty without your job phone and use the camera on your own device to take photographic evidence, the image/s will need to be uploaded to Evidence .com. Once that has been completed satisfactorily the images should then be wiped from your device.

So to re-cap, only in extreme circumstances should you resort to using your personal device for policing purposes. These will usually cover the following circumstances:

- extreme, matters of urgency which you must be able to justify
- Incidents that occur whilst off duty
- when you don't have access to any Met communications device

**14. What are the risks of unlawful / inappropriate use of Met information/ IT systems?**

It is important to know that inappropriate use, access or disclosure of any Met/ national policing information or of ICT systems is a disciplinary matter that may also constitute a criminal offence. It could lead to disciplinary or criminal proceedings due to misconduct or gross misconduct. Met information should only be accessed where there is a policing purpose and on a strict need to know basis. In all circumstances, you must be able to justify your actions carried out on your Met account as being acceptable and in accordance with corporate policy.

**15. What adverse data, systems and communication issues have arisen?**

The sharp rise in discipline cases has fairly frequently involved the most serious forms of online misconduct perpetrated by some of our staff, which has then brought the Met into disrepute. Some of this has involved a significant amount of misconduct activity that has been perpetrated using privately owned devices, but sometimes it has involved use of Met ICT systems/ devices. Either way, the damage caused to the Met, UK policing generally and above all the public has had a profound impact on the ethos of UK policing by consent. The clear message is that online communications misconduct, featuring abuse/ discrimination and harassment of the public, partners or colleagues will not be tolerated and individuals will be held fully accountable. This includes misuse of social media/ instant messaging or posting distressing/ inappropriate images/ material online, something which is never permitted or justifiable. Furthermore, unauthorised data

searches and unwarranted personal data disclosure is also unlawful. Any such unauthorised or illegal activity profoundly damages the Met. It will almost certainly result in regulatory censure, enforcement action and fines imposed by the Information Commissioner.

**16. How can I access Met information/ ICT systems without breaching professional standards?**

- Ensure that whenever you view, share or amend Met information, you have a justifiable policing purpose for doing so. This means, that when searching on a Met intelligence system, you do so as part of your investigations or work duties. Having access to a system, does not entitle you to freely conduct searches without a legitimate policing purpose connected to your specific duties. Likewise, acting on your interest, out of curiosity, personal desire or on behalf of others, is something that is strictly not permitted.
- Both you and the individual/s you are sharing Met information with, must have a legitimate or policing need to know, so be particularly mindful when disclosing Met information with those persons outside the policing organisation.
- To help secure the information, ensure it is always stored correctly and on the right system according to Data Protection Act 2018/ UK GDPR and MOPI requirements. The same degree of protection must be afforded to the storage of important original paper documents that are considered of evidential value or are corporate records [e.g. registered files]. Such papers must not be destroyed without authority and should be archived in the correct corporate repository.
- Limit your use of Met devices for personal reasons to those exceptions found in the Use of MPS ICT Systems Policy, ensuring that it's occasional and does not interfere with your policing duties [see also FAQs 10 – 12 above].
- Avoid using your personal device for policing business, unless in extreme, urgent circumstances or where you're unable to access a Met phone, tablet or laptop.
- Remember, all Met systems and phones will be monitored so you will need to be able to fully justify your actions on your accounts at all times.

**17. What happens if the re-issued policy, rules and guidance is not followed?**

The policy is not designed to punish honest mistakes, but it has to be clear and robust regarding situations where there is evidence of individual behaviour that is completely unacceptable. This is where individuals contravene police regulations, professional standards and the policing code of conduct. Prima facie such behaviour and activities will constitute either misconduct or gross misconduct under the discipline code. It will therefore result in discipline or criminal sanctions for any Met personnel involved, including potentially dismissal from the police service. Furthermore, any staff that 'look the other way' and who fail to acknowledge, challenge and report unacceptable conduct by colleagues may also face censure.

**18. What does the Met do to protect Met data, data systems and communications?**

As one might expect, organisationally our systems are security assured and the Met SEG [security firewall] has technical controls and web filtering to protect the external interface and online services [like the Internet] from cyber-attack and infiltration. Despite such measures, the Met still expects all authorised users to follow security guidance in relation, say to suspicious emails, to report security incidents, but also to understand that all our systems and communications are publically accountable and therefore subject to lawful monitoring and audit to ensure data CIA is maintained. This means that there can be no expectation of privacy for anyone using policing systems. You must at all times conduct yourself professionally using systems or telephony, as it is highly likely your interactions have been recorded and you may have to justify yourself at a later date. Since the beginning of 2023, an enhanced lawful business monitoring (LBM) capability has been introduced. It should therefore now be assumed that all systems and communications will be monitored on a 24/7/365 day basis.

**19. What should I do if I become aware of a security breach?**

If you become aware of a suspected breach or misuse of Met information, systems or ICT devices, you must report it as a security incident. Recent data breaches by policing have been high profile and widely reported in the national media. Other examples could include someone using a personal phone to take screenshots of sensitive information held on Met systems, posting distressing or evidential crime scenes images on social media or sharing Met data with those without a need to know. Reporting is not about attaching blame, as many incidents are inadvertent; or might be due to an external cyber-attack [e.g. ransomware], other technical or process failure. Initially establishing the facts regarding scope, depth and potential impact of the data breach or other security incident is the most important factor. Time is of the essence as risk assessment will need to be made and an opportunity for early mitigation of such risk might be available if reported promptly. The most serious data breaches will need to be escalated and reported to the Information Commissioner, so you must report the incident to the Information Assurance Unit – Data Office (DDaT), as soon as possible, or no later than 12 hours of becoming aware of the incident to ensure that the statutory time limit is met under the Data Protection Act 2018.

To access the online security incident reporting form, visit Report a security incident on the Intranet homepage or Stay Alert. Otherwise, you can learn more about security incidents at Guidance on security incident reporting.

**20. Who has approved the policy changes?**

Management Board unequivocally supports this corporate policy change as it provides a firm foundation to help address the risks posed by any unlawful, inappropriate or unauthorised use of Met data, data systems and communications. It is expected that this should help towards achieving an improved working culture and environment.

Therefore, everyone in the Met is obliged to comply with the refreshed policy requirements, rules and guidance, to ensure continued confidentiality, integrity and availability (CIA) of Met data, plus appropriate use of technology supporting primary policing purposes

## 21. Where else can I find more information?

These FAQS support publication of the latest published versions of the **MPS Information Code of Conduct** and **Use of MPS ICT Systems Policy**. If there is anything you are not clear about initially after reading these documents please discuss any issue with your supervisor or line manager.

To view information management and security documentation please go to:
Information Management policies
For Digital Policing support see
http://mpsweb.intranet.mps/support/digital_experience/ and
Professional standards see - http://mpsweb.intranet.mps/policing/professional-standards/

**Policy owner:** Aimee Smith, Data Director & Head of Profession for Darren Scates, Chief Digital, Data & Technology Officer.

**MPS Senior Information Risk Owner (SIRO):** AC Barbara Gray, Head of Professionalism.

**Content owner:** [redacted] Higher Information Assurance Manager [Policy Developer], reports to [redacted] [MPS Information Security Officer (ISO)] and Darren Curtis, MPS Data Protection Officer and Head of Information Law & Security – Data Office (DDaT).