MOPAC | MAYOR OF LONDON
OFFICE FOR POLICING AND CRIME

OVERALL POLICY AIM

MOPAC guidelines for all staff accessing MOPAC email service, calendar, GLA/MOPAC network and other technology services using a Corporately Owned (CO) mobile device, laptop or Surface Pro.

IT Acceptable Use Policy

MOPAC is increasingly using mobile devices, laptops and Surface Pros to access corporate information on MOPAC IT systems and services. To assist, TG offer a robust service which allows members of staff to access their MOPAC email, files and the GLA Intranet (including access to CONNECT) from these devices.

This document sets out the risks and the security measures in place to protect MOPAC information, the acceptable use of MOPAC and GLA data, mobile and IT assets, and guidance from the GLA acceptable usage policy.

Scope

In this policy "staff" includes contractors, agency workers, office holders, secondees and volunteers engaged by MOPAC.

Definitions

1. A CO device means that MOPAC owns the device and Technology Group (TG) maintain and support them. As a result, TG will have complete control over a MOPAC CO device.

2. MOPAC defines acceptable use as activities that directly or indirectly support the business of the organisation.

The risks

3. There are a number of risks to MOPAC and the GLA in the use of mobile devices. Loss of a device, data being accessed by an unauthorised person and misuse of devices all pose a threat to MOPACs effectiveness, reputation and data security.

4. The conditions of use and acceptable use in this document sets out measures to mitigate these and other risks. It is the responsibility of staff to ensure that they comply with this policy. A failure to do so, which results in professional or reputational damage to MOPAC could constitute a disciplinary offence.

5. Central to the guidance we provide is that you clearly understand your responsibility and are guided by a number of official points-of-reference. The Information

Commissioner's Office (ICO) guidance states data security is a prime concern for employers and importantly mobile devices, laptops and Surface Pros should not introduce vulnerabilities into existing secure environments.

6. The Data Protection Act (DPA and GDPR) states employees must take measures against unauthorised or unlawful processing of personal data and the Employment Practices Code states that employees are entitled to a degree of privacy in the work environment. Further personal guidance is also available on the Getting safe on line – Smartphones and Tablets site.

7. In line with the advice and guidance above, TG offers access to O365 on the MS Cloud, Citrix which provides remote access to MOPAC network drives, SharePoint, and the GLA Intranet (including CONNECT) to MOPAC CO iphones, laptops and Surface Pros.

8. MOPAC data is security ring-fenced to ensure that if any CO device is lost or stolen the data is kept confidential by:

    a. Iphones - incorporating conditional access, Multi-factor Authentication (MFA) and having restrictions in place such as blocking airdrop, pairing with apple watch, multiplayer gaming, movies, and transferring of corporate contents to unmanaged applications. To enhance the security MS Intune is installed to prevent staff from downloading the Outlook app in the Apple app store from any other phone device.

    b. Laptops and Surface Pros – installing MS BitLocker to further safeguard our data by rendering the information stored on them inaccessible if they are lost or stolen.

9. In addition to the security measures on devices, the following are also in place:

Email encryption

10. All MOPAC outgoing emails are encrypted to the government recommended standard of Transport Layer Security (TLS) Protocol 1.2*. TLS is an industry standard designed to protect the privacy of information communicated over the Internet.

11. If the recipient uses commercial email applications such as Microsoft like we do, emails will be encrypted to this standard. However, if they use lesser known shareware/freeware mail applications and it is detected that it doesn't support TLS 1.2, the outgoing email will not be encrypted.

Antivirus

12. CrowdStrike is the anti-virus system used to protect MOPAC and the GLA from malicious cyber-attacks on our laptop and Surface Pro devices.

The legal framework

13. All the legal obligations, rights and responsibilities that apply to staff using MOPAC/GLA IT systems, services and data at MOPAC's office locations will apply to the use of mobile devices, laptops and Surface Pros.

Acceptable use

14. When using your CO mobile device, laptop or Surface Pro you must abide by MOPAC's values, policies and the following rules whether working on or offsite:

    a. **Be Lawful** – Do not act in any way that could be unlawful or encourage others to act unlawfully. In particular, do not infringe intellectual property rights, do not reveal confidential or sensitive information and do not engage in any criminal offence or encourage others to do so. Comply with the applicable legal and regulatory policies at all times.

    b. **Be Responsible** – You must not undertake actions that are harassing, defamatory, threatening, obscene, abusive, racist, sexist, offensive or otherwise objectionable or inappropriate. Do not pretend to be anyone other than yourself when online.

    c. **Be Reasonable** – Do not use the access in any way that may affect the running of the GLA network or other technology connected to it or devices.

    d. **Be Protective** – Keep your device and software up to date. Do not install software other than from reputable sources. When in public places, do not use your iphone, laptop or Surface Pro in a way that increases the likelihood of theft. Do not share your CO device with others, which may give them access to MOPAC data. Do not connect to unsecured networks (including wired) which don't require you to input a password. You can set up a personal hotspot with your corporate iphone by tethering it to your laptop or Surface Pro which will ensure a secure and safe wifi connection.

    e. MOPAC devices are not provided for personal use by you or anyone else.

    f. Access to corporate emails or MOPAC systems is not permitted from personal devices without logging in remotely via Citrix. MOPAC data, information and emails should not be transferred or forwarded to personal devices or emails accounts.

    g. Only trusted apps for business use only from reputable sources should be installed.

    h. Your devices will be set to auto install the latest security and operating system upgrades – this must not be turned off.

    i. Secure your iPhone by using a unique password 6-digit password or a biometric access control (e.g. fingerprint scanner or facial recognition).

    j. Configure your iPhone, laptop or Surface Pro to automatically lock after being left idle for a set time of no more than 5 minutes. Lock your iphone, laptop or Surface Pro whenever you are not using it or move away from the device.

    k. Protect your device and take all measures necessary to keep it safe when working in the office or remotely, travelling and stored away. Protective sleeves or cases can be provided on request if required.

l. Lock your laptop or Surface Pro in your hotbox at the end of each day and store in your team's allocated tambour storage unit if not taking home with you.

m. Be aware of the risks when using your device outside the office or home. Use a privacy screen cover if necessary. It is your responsibility to ensure that MOPACs information is kept safe.

n. Inform the Technology Group Service Desk ([redacted] Monday – Friday, 8.00-18.00 or out of hours [redacted]) if your device is or suspected to be lost or stolen as soon as practicably possible so that appropriate steps can be taken to remotely delete the MOPAC email account and other data belonging to MOPAC from the device.

15. If in doubt or concerned that you may have inadvertently breached this policy or are concerned about a potential security breach, please contact the Data Protection Officer (DPO) James Bottomley to seek advice during normal working hours.

16. Use of your device for MOPAC services is regulated by various UK Laws, and it is your responsibility to familiarise yourself with their requirements. These laws include: Data Protection Act 1998 (DPA 1998) - Computer Misuse Act 1990 - Trade Marks (Offences and Enforcement) Act 2002) - Data Retention (EC Directive) Regulations 2009 - Digital Economy Act 2010 - Freedom of Information act 2000

17. Breaches of this policy may result in disciplinary action being taken against you in accordance with MOPAC Disciplinary policies and procedures. With regard to contractors, agency workers, etc. breaches of this policy may lead to termination of your contract.

Agreement

18. By agreeing to use a CO mobile device, laptop or Surface Pro you are accepting the terms of this policy.

Policy Review Log

Version	Date	Author	Description of change
0.1	12/10/2017	[redacted]	First draft
0.2	27/11/2018	[redacted]	Adapted acceptable use list
0.3	18/03/2019	[redacted]	Added opening paragraph. Added detail on anti-virus Added detail on email encryption.