Metropolitan Police Authority

IS/IT Department

Information Security Policy

Version 1.2

This is a high level policy on acceptable usage and best practice for internet browsing, email, remote access, wireless connectivity and personal digital assistants. The incident reporting process is also detailed.

All authorised users of MPA technologies are required to read and sign up to this policy before access is granted.

This is a continuously evolving policy and as such is subject to change. The current version of this policy can be obtained from HR, IS/IT, or your line manager.

Table of Contents

1. INTRODUCTION

The purpose of this document is to ensure that all users of the Metropolitan Police Authority (MPA) systems are fully aware of what they are permitted to do and what is not allowed. The intention is that it will remove any ambiguity that exists.

It has been produced to also provide protection to the MPA staff members and the MPA in defining what is acceptable.

The primary purpose of the MPA is to conduct our business: anything that interferes with that will not be permitted. However, it is important that members of staff do have a certain amount of flexibility providing it does not impact with the day-to-day running of the Business.

In the event of any queries, these should be raised with your line manager or Department Head in the first instance.

It is likely that these policies will be reviewed and updated periodically and you will be issued with a revised copy accordingly.

The last section of this document is a consent form. By signing this, you are stating your agreement to adhere to the controls and policies that are defined within this document.

2. EMAIL

2.1. Purpose

To prevent tarnishing the public image of the Metropolitan Police Authority (MPA) and to maintain good Information Security practices. When email goes out from the Metropolitan Police Authority the general public will tend to view that message as an official policy statement from the Metropolitan Police Authority.

2.2. Scope

This policy covers appropriate use of any email sent from an MPA email address and applies to all Members, officers, contractors, and agents operating on behalf of the MPA.

2.3. Policy

2.3.1. Prohibited Use

The Metropolitan Police Authority email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, physical appearance, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any MPA employee should report the matter to their line manager immediately.

2.3.2. Personal Use

Using a reasonable amount of Metropolitan Police Authority resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from an MPA email account is prohibited as is the distribution of non-work related attachments. Virus or other malware warnings and mass mailings from the MPA shall be approved by MPA IS/IT Department before sending. These restrictions also apply to the forwarding of email received by a MPA employee.

2.3.3. Monitoring

Metropolitan Police Authority employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. The MPA may monitor messages without prior notice. Technology components are in place to prevent the delivery of email (both internal and external) which is considered to be offensive. In some cases, this will be based on words used within the email. Due to the nature of our work, it is acknowledged that this may in some instances cause a problem. Any such problems should be referred to the IS/IT Helpdesk in the first instance.

2.3.4. Anti-Virus

Users should have an anti virus program installed on their computers. Real time system scans should be enabled. The anti-virus scanner's definition should be updated regularly. For those users who are connected to the network, there is an automated process to facilitate this. For remote users, this is discussed later within this policy.

2.3.5. Attachments

Attachments are one of the primary delivery vehicles for viruses and worms. Hence, users should be very careful when opening attachments from unknown senders. As email addresses can easily be spoofed, users should also be careful when opening attachments from trusted sources. Attachments with executable content should not be opened.

2.4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

2.5. Definitions

Term	Definition
Employee	Any Member, officer, contractor or agent operating on behalf of the MPA.
Email	The electronic transmission of information through a mail protocol such as SMTP, POP3 or IMAP. The only MPA supported email client is Microsoft Outlook.
Forwarded email	Email resent from an internal network to an outside point.
Chain email or letter	Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.
Sensitive information	Information is considered sensitive if it can be damaging to the Metropolitan Police Authority, and/or its stakeholders' reputation or standing in the Community.
Virus warning	Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.
Spoofed	This is where the email address that the message purports to come from is not actually the real email address. For example, you may receive and email from administrator@mpa.gov.uk, but the real originator will be a completely different address.
Unauthorised Disclosure	The intentional or unintentional revealing of restricted information to people, both inside and outside the Metropolitan Police Authority using email, who do not have a need to know that information.

3. INTERNET USE

3.1. Purpose

This policy defines appropriate Internet Policy.

3.2. Scope

This policy covers all Internet usage whether for professional or personal use on the Metropolitan Police Authority network and applies to all employees, contractors, and agents operating on behalf of the Metropolitan Police Authority.

3.3. Policy

3.3.1. General Use

For the most part, the Internet should be accessed for work related activities, and you should exercise common sense to ensure that you avoid web sites that contain inappropriate and offensive material. Occasional personal use is acceptable, but this should be done using discretion and must not interfere with your normal day-to-day duties.

3.3.2. Inappropriate Use

Users should not access web sites which are deemed inappropriate such as pornographic web sites, web-based email sites, online gambling sites, and job advertisement sites. If in doubt whether Internet use is appropriate, contact the IS/IT Helpdesk via email.

3.3.3. Web Mail & Internet Chat Rooms & Instant Messaging

Access to Internet Chat Rooms, Instant Messaging and web mail, such as Yahoo and Hotmail is prohibited to avoid potential information leakage and to stop malicious code and viruses entering the MPA network.

3.3.4. Program Downloads

Many programs contain spyware and sometimes even malicious code. Hence, programs should not be downloaded and executed without the consent of the MPA IS/IT Department.

3.3.5. Exceptions

Users are allowed to access inappropriate sites & Chat Rooms if it is required to fulfil their job function. However, access to such sites will have to be requested via email from the IS/IT Helpdesk.

3.3.6. Technical Controls

The IS/IT Department have implemented controls that will restrict which web sites users are permitted to visit as well as scanning the content of downloaded content for the presence of malicious code. All Internet access activity is logged; this includes the user name, date/time and the URL address visited (e.g. www.bbc.co.uk). This applies to both successful and failed attempts to access a website.

3.4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

3.5. Definitions

Term	Definition
Internet	The Internet is the publicly available worldwide system of interconnected computer networks that transmit data by packet switching over the Internet Protocol (IP). It is made up of thousands of other; smaller business, academic, and government networks that provide various information and services, such as by electronic mail, online chat, and on the graphical, interlinked World Wide Web.
Web Mail	Email that is accessible via a standard web browser.

4. PORTABLE DEVICES

4.1. Purpose

This policy defines the security precautions to be taken when using portable devices such as PDAs, USB drives, wireless devices and so on.

4.2. Scope

This policy covers all portable devices, which have any MPA data stored on them.

4.3. Policy

4.3.1. Specifications

Portable devices can store a large amount of data nowadays. If a PDA is stolen or lost and no proper safeguards have been implemented, the information stored on it can be at risk. Such an incident can represent a major security breach. Hence, only portable storage devices that have the following facilities will be considered for MPA approval:

- The ability to impose an MPA approved password mechanism;
- The ability to ensure that synchronisation can only be undertaken with authorised terminals;
- The ability to automatically encrypt the total contents of any external memory storage cards (SD, compact flash, XD, memory stick or smart media);
- The ability to enforce centralised control over and remove user control of programs/applications and functions on the PDA including use of infra-red data ports, blue-tooth or other wireless connectivity;
- The ability to lock the device or erase its contents after a pre-determined number of failed password attempts.

4.3.2. Connection & Use Limitations

Portable devices, by virtue of the data stored within, should be afforded the same level of physical security protection normally assigned to assets elsewhere with an equivalent marking. The connection of portable devices to any system that holds or processes information protectively marked confidential or above is prohibited.

PDAs shall not to be taken into any room where material marked confidential or above is discussed, even when switched off as many have the facility to act as recording devices and may well be able to re-transmit any conversation.
The connection of any portable devices not furnished through the MPA IS/IT Department is prohibited.

Any on-board long-range communications (e.g. GSM, GPRS, WAP etc) must be disabled whilst connected directly to any MPA network systems, whether or not it is standalone, LAN, WLAN or WAN.

Where a portable device is connected via a direct remote connection the device must have installed encryption software of a baseline standard, to provide secure communications between the portable device and the MPA system(s). When any such connection is made it should only be for a limited period of time sufficient to synchronise email and other information and the device should then be disconnected.

4.3.3. Data/Information Storage & Processing

MPA information protectively marked up to RESTRICTED, data requiring the PRIVATE descriptor which identifies any information requiring protection under the Data Protection Act 1998 may be stored on a MPA furnished compliant Portable Device.

Users are permitted to use their own PDA's at work. However, it must not be connected and/or synchronised with any machine and must not store any MPA related data.

In the event of the PDA being lost or stolen, it must be reported to the nearest Police station and both the Admin/Finance Department and the IS/IT Department.

To protect the data / information assets of the MPA, where data up to RESTRICTED is stored they must be encrypted on any memory card.

4.3.4. Disposal of PDAs

The PDA can be considered in this case as a hybrid of RAM memory, and a laptop where the solid-state memory cards (SD, Compact Flash, XD, smart media or memory stick) are analogous to the laptops hard disk. The disposal procedures must ensure that either:

- ♦ All data is effectively wiped from the device or
- ♦ All removable memory/media is destroyed;
- ♦ The Device is reformatted;
- ♦ Operating system software is refreshed.

Where protectively marked data up to RESTRICTED has been permitted, the data files are to remain encrypted whilst the procedures above are carried out during disposal.

4.4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. WIRELESS COMMUNICATION

5.1. Purpose

This policy prohibits access to Metropolitan Police Authority networks via unsecured wireless communication mechanisms whether it is at the office, from home or from any another location.

5.2. Scope

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of Metropolitan Police Authority's internal networks. In instances where MPA computing facilities have been installed or are used at a member or officers' home, this will be considered to be an extension of the MPA network as far as wireless devices are concerned. This includes any form of wireless communication device capable of transmitting packet data.

5.3. Policy

5.3.1. Access Points and Cards

At the current time, no wireless access points or devices are permitted within the MPA premises. Any PC's that have inbuilt wireless capabilities will have such features deactivated. These must not be re-activated.

Where a member or officer works from home on any basis and connects to the MPA using an MPA laptop or PC, the following will apply:

- ♦ If access is via a Broadband router, the wireless element of this must be disabled.

Whilst it is accepted that this may not be possible, the laptop will be configured with a personal firewall that will deny access to any machine that attempts to connect to it. If a home PC (i.e. non-MPA machine) is connected to the broadband switch at the same time as the MPA machine, you have in effect created a local network at home of which your MPA machine is part. Under no circumstances must any data be transferred from your MPA machine to your home machine and vice versa.

Only MPA issued printers can connect directly to MPA laptops and PCs. No other printers will be supported. Personal printers and any other non-MPA printer should not be connected either directly "locally" or via a network.

5.3.2. VPN Encryption and Authentication

All computers with wireless LAN devices must utilise an MPA approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic. To comply with this policy, wireless implementations must maintain point to point hardware encryption of at least 128 bits. The encryption keys should be changed on a regular basis. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address. All implementations must support and employ strong user authentication, which checks against an external database (RADIUS).

5.3.3. Setting the SSID

The SSID (a SSID is the name of a wireless local area network (WLAN). All wireless devices on a WLAN must employ the same SSID in order to communicate with each other) shall be configured so that it does not contain any identifying information about the organisation, such as the company name, department title, employee name, or product identifier.

5.4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.5. Definitions

Terms	Definitions
User Authentication	A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

6. REMOTE / MOBILE WORKING

6.1. Purpose

The purpose of this policy is to describe the responsibilities of both the organisation and individuals in ensuring the protection of MPA computer systems and paper records when working remotely.

6.2. Scope

This Policy applies to all authorised remote users of the MPA IT infrastructure and those who have access to MPA paper files. This includes MPA employees, temporary staff, contract staff and consultants.

This policy is based on a requirement that an assessment has been conducted as to the requirement for remote working to take place. The assessment should consider aspects such as the financial costs, the additional security risks and Health and Safety issues relating to the remote working.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, broadband and cable modems.

6.3. Policy

6.3.1. General

Remote workers need to be extra vigilant as they face more threats than workers at the office who operate in a controlled environment. Hence, they must implement the right security measures to protect MPA information. It is the responsibility of MPA employees and agents with remote access privileges to MPA's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to MPA.

General access to the Internet for recreational use by immediate household members through the MPA Network on personal computers is prohibited.

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of MPA' network:

a. Email Policy
b. Internet Use Policy
c. Use of Portable Devices Policy
d. Wireless Communications Policy
e. Escalation and Incident Reporting Policy

6.3.2. Transit and Storage of Information

The Transit to, or storage at, remote locations of MPA Information (including electronic documents stored on a mobile device) must comply with the appropriate handling requirements for the information based on it's protective marking.

6.3.3. Use of Computers in Public Places

Extra precautions have to be taken when a computer is used in a public place such as on a train for example. To avoid shoulder surfers the user should make sure that no one can see him/her typing his/her username and password. No sensitive material should be accessed in public places.

6.3.4. Requirements

Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication followed by the network user account / password combination.

At no time should any MPA employee provide their login or email password to anyone, not even family members. If it is required by the IS/IT Department, they will request it personally, though they have the ability to change it. If in doubt, do not disclose your user account and password details to anyone.

MPA employees and contractors with remote access privileges must ensure that their MPA-owned or personal computer or workstation, which is remotely connected to MPA's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user (i.e. via a broadband switch).

MPA employees and contractors with remote access privileges to MPA's corporate network must not use non-MPA email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct MPA business, thereby ensuring that official business is never confused with personal business.

Reconfiguration of a home user's equipment for the purpose of split-tunnelling or dual homing is not permitted at any time. This will ensure that all communication will be sent to the MPA only and will not be routed to the Internet directly.

All PCs and laptops connecting to the MPA internal network via remote access technologies must use the most up-to-date anti-virus software. This includes personal computers and laptops. Third party connections must comply with requirements as stated in the Third Party Agreement.

Personal equipment that is used to connect to MPA's networks must meet the requirements of MPA-owned equipment for remote access. The MPA does not support any non-MPA PCs, laptops, network or any other devices or technologies irrespective of whether it is used to conduct MPA business.

6.4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.5. Definitions

Term	Definition
Cable Modem	Cable companies such as Telewest Broadband provide Internet access over Cable TV coaxial cable. A cable

Term	Definition
	modem accepts this coaxial cable and can receive data from the Internet at over 4 Mbps. Cable is currently available only in certain communities.
CHAP	Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCI Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.
Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analogue signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the corporate network via a local Ethernet connection, and dialling into AOL or other Internet service provider (ISP). Being on a MPA-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into MPA and an ISP, depending on packet destination.
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
ISDN	There are two flavours of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signalling info.
Remote Access	Any access to MPA's corporate network through a non-MPA controlled network, device, or medium.
Split-tunnelling	Simultaneous direct access to a non-MPA network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into MPA's corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunnelling" through the Internet.

7. ESCALATION AND INCIDENT REPORTING

7.1. Purpose

This policy defines appropriate escalation and incident reporting procedures.

7.2. Scope

This policy covers all the escalation and incident reporting procedures for the Metropolitan Police Authority network and applies to all employees, contractors, and agents operating on behalf of the Metropolitan Police Authority.

7.3. Policy

7.3.1. Incident Identification and Reporting

The first stage in the Incident Handling Process is the correct identification of security incidents.

There are a wide variety of events that are pertinent to the MPA. Typical examples are listed below.

- Malicious code attacks (viruses, worms, etc);
- Network Attacks;
- Probes, scanning, etc (should be reported only if they consume significant resources);
- Denial of Service (DOS);
- Inappropriate use;
- Hoaxes (should be reported only if they consume significant resources);
- Unauthorised Access;
- Compromise of Integrity;
- Spoofed News stories;
- Email abuse.

Incidents must be identified and reported immediately to the IS/IT Helpdesk irrespective of what you consider the seriousness or implications to be. Judgement will be required to differentiate between a genuine incident and a glitch in the network and/or systems.

7.3.2. Incident Management

The process of managing an incident includes all the activities connected with the technical features of analysing and investigating the incident, fixing software, hardware, as well as the Metropolitan Police Authority's response to external organisations such as the media. It is likely that with some incidents a co-ordinated effort with one or more authorities will be required. The likely consequences of each incident must be assessed and updated, as information becomes available. In all instances, the IS/IT Helpdesk or the respective Department Head must be advised as soon as an incident has occurred.

7.3.3. Severity Levels

Incidents will be categorised as one of four severity levels. These levels are based on the impact to MPA's operation. In order to identify the scope and impact, a appropriate set of criteria should be defined.

Factors to consider include but are not limited to:

- Is this a departmental or organisation-wide incident?
- Are many computers affected by this incident?
- Is sensitive/confidential information involved?
- What is the entry point (workstation, network etc) of the incident?
- What is the potential financial impact to the MPA?
- What is the potential impact to the reputation of the MPA?
- What is the potential damage of the incident?
- What resources could be required to handle the incident?
- What is the estimated time to close out the incident?
- What are the wider reaching implications of this incident?
- Loss of Operations etc.

However, the following examples should assist in showing the sort of incidents each level might indicate:

- Level 1 - unauthorised use of a critical application user id, compromise of a high privilege system account, theft of important equipment, local fraud, compromise of a critical multi-site application, break in on the router network;
- Level 2 - proliferation of a computer virus across multiple workstations, unauthorised use of the mail network;
- Level 3 - computer virus incident (non-destructive), unauthorised use of a file server account;
- Level 4 – local virus (no impact), unauthorised use of non-critical file server account.

Impact analysis should take place with reference to local department processes and service(s) affected. Contact should be made with the appropriate Head of Department to help determine the possible organisational impact. There should be an informed trade off between under-reaction (suffer the consequences) and over-reaction (waste time and resources unnecessarily).

7.3.4. Incident Closure

An incident can only be closed when it has been properly investigated and is deemed not to present an unacceptable threat to Metropolitan Police Authority systems and that the Press Office are adequately equipped to deal with any questions that they may receive.

7.3.5. Incident Review

Incidents must be recorded and reviewed on a regular basis by the MPA Senior Management Team to ensure that they have been dealt with, and to detect any trends or anomalous activities.

7.4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7.5. Definitions

Terms	Definitions
Data	This term covers all types and forms of data that can be handled by IT systems. For example, data can take the form of text, image, spreadsheet, or graphics.
Hardware	Hardware is the physical units making up the IT system.
Software	Software is a term used to refer to all programmes pertaining to the operation of an IT system.
Incident	An incident is an event where a there has been a breach of the confidentiality, integrity or availability of any information under the control of the area.

8. INFORMATION SECURITY POLICY SIGN OFF DOCUMENT

The Metropolitan Police Authority employees and authorised users shall have no expectation of privacy in anything they store, send or receive on the Metropolitan Police Authority's email and information systems.

The Metropolitan Police Authority may monitor messages and data communications without prior notice in accordance with the Data Protection Act to ensure compliance with the Information Security Policy.

I have read the MPA Information Security Policy and agree to abide by it. I understand that violation of the Policy may result in disciplinary action being taken against me.

The Information Security Policy is continuously evolving. As such, I may be required to sign off future revisions of this policy. I understand that violation of this Policy may result in disciplinary action.

Name (print) ______________________________

Position: ______________________________

Department: ______________________________

Signature: ______________________________

Date: ______________________________