Title & Version	Information Code of Conduct, Version 3
Contact Point	Information Compliance, DoI 2(3), (020) 7091 5084 (Internal Network 78-5084)
Location	Room 1 East, Edinburgh House
Summary	The Information Code of Conduct sets out the policy on the use of MPS information and information, communication and technology systems

INFORMATION CODE OF CONDUCT

VERSION 3 – August 2007

METROPOLITAN POLICE Working together for a safer London

INTRODUCTION

Information and intelligence leakage poses a significant and growing threat to the operational effectiveness of the MPS. Misuse of MPS information and information, communication and technology systems may result in the loss of public confidence in our ability to safeguard information.

This code of conduct summarises Service policy on the use of MPS information and information and communication systems. You should be aware that instances of misuse might result in disciplinary action and may constitute a criminal offence.

USE OF MPS INFORMATION

Only use information for official policing purposes that constitute part of your public duty. This covers information in all formats e.g. text, images, photographs and videos.

Use for personal purposes is *strictly forbidden* - This includes using MPS information within blogs on the internet.

You cannot access information for personal or family reasons. If you believe you may be in that situation you must bring the matter to the attention of your line management.

Only share information with those with a genuine 'need to know'. Check with your line management or information manager if you are in any doubt before releasing any information.

Only use and disclose information in accordance with legislation e.g. Data Protection Act, 1998 and the Freedom of Information Act, 2000.

The statutory Code of Practice on Management of Police Information 2005 defines 'police information' as "information for a policing purpose" (e.g. crime and public protection).

Police information is a corporate resource and must be searchable and retrievable by those that need to use it for official purposes. Unless officially sanctioned to do otherwise by management you must store police information in the relevant 'corporate repository' (i.e. MPS file plan, registered file, or key MPS system, e.g. CRIMINT). You must not store police information where it cannot easily be searched for and retrieved. Police information input or processed in non-corporate systems (e.g. in locally developed spreadsheets/databases, in your AWARE 'home directory', or on stand alone computer), must be transferred into the corporate repository at the earliest opportunity.

Email is not a corporate repository it is a communication tool. Police information that needs to be retained must be stored in the relevant corporate

repository, rather than as the contents of an email in your inbox or other Outlook folder.

Only share information with those with a genuine 'need to know'. Check with your line management or information manager if you are in any doubt before releasing any information.

Only use and disclose information in accordance with legislation e.g. Data Protection Act, 1998 and the Freedom of Information Act, 2000. Your local information manager will be able to either advise you on this in the first instance, or refer more complex issues to the Public Access Office, DoI2(3-3).

USE OF MPS INFORMATION, COMMUNICATION AND TECHNOLOGY SYSTEMS

You **must not**, unless your duties require you to do so:

- Create, adapt, view, display or transmit any material that is defamatory, racist, sexually explicit or pornographic, sexist, homophobic, religiously offensive, illegal, in breach of the MPS diversity and equal opportunities policies or otherwise offensive.
- Open, execute, store or install onto any MPS information system, transmit or solicit from others any software or executable files.
- Create, adapt, store, view or transmit any malicious code (e.g. a computer virus or worm)

You **must not** under any circumstances use any information, communication or technology system for personal business reasons.

The only information, communication, and technology systems in relation to which any personal use will be permitted are the Metphone telephone system, mobile telephones, facsimile (fax) machines, Microsoft Word, Excel and Outlook (email) on AWARE.

Only a very limited and reasonable amount of personal use will be permitted [see Personal Use of MPS Information, Communication and Technology Systems SOPs on the Information Management website for details].

The use of any other MPS or national information system for personal purposes is *strictly forbidden* and may lead to disciplinary action. It may constitute a criminal offence.

PROTECTIVE MARKING

You **must**:

- Mark information in accordance with the Protective Marking System. Information not requiring a protective marking should be marked Not Protectively Marked.

- Ensure information is stored, circulated and disposed of in accordance with the protective marking.

ACCESS CONTROL

You **must**:

- Protect your password(s) to information systems.
- Log off before leaving a workstation. You are accountable for actions undertaken under your user identity.
- Ensure information is appropriately secured when offices are left unattended.
- Limit access to all information on a 'need to know' basis.

MONITORING AND AUDIT

It should be noted that as part of the proper management of the MPS, its public functions and its resources, it is necessary to monitor information systems to the extent permitted by law. On occasions this may result in the deletion of information.

Details of the web pages you visit are recorded and may be audited.

The monitoring and recording of communications will only be used where the level of intrusion is proportionate to the matter under investigation or evaluation.

You **must** report incidents of misuse or security breaches to your line management.

Information Code of Conduct Acknowledgement Form

1. I have read, understood and undertake to comply with the Metropolitan Police Service (MPS) Information Code of Conduct.

2. I understand that misuse of MPS information or any information, communication or technology system may result in disciplinary or criminal proceedings.

Signature: Date:

Name:

Rank / Appointment:

Warrant / Pay No: