ICT Acceptable Use (Policy)

OFFICIAL

Publication Scheme Y/N	Policy section can be published on Force Website Procedure should be withheld
Department of Origin	Corporate Support & Development (CSD)
Policy Holder	Head of CSD
Author	Information Assurance Coordinator (CSD)
Related Information	Computer Misuse Act Data Protection Act Freedom of Information Act Government Protective Marking Scheme/Government Classification Scheme Official Secrets Act Police and Criminal Evidence Act Records Management Procedure Regulation of Investigatory Powers Act Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations
Date Approved at FPG	25/04/2012
Previous Version	Version 3.2 – Created 10/11/2020
This version	Version 3.3 – Created 27/05/2022
Date Approved at SMB	29/06/2022
Date of Next Review	27/05/2025

June 2022

Contents

Version History

Version Number	*Date*	*Rational behind amending/updating policy or procedure.*	*Policy Owner details*
V.2.0	20/07/2016	V 2.0 – Major rewrite to subsume and consolidate other Information Assurance related policies (Email & Electronic Messaging, Handheld Devices, Mobile Devices, Mobile Phones, Internet & Remote Working). Approved at SMB 20/07/2016	Head of CSD
V.3.1	07/01/2020	V3.1 –A number of amendments have been added to procedures to cater for changes in systems and technologies. Sections have been added for social media (8.6) and Body Worn Video Devices (13). The Remote Working (7) and Monitoring (17) sections have been rewritten.	Head of CSD
V.3.2	10/11/2020	V3.2 – Amendments to section 5.6 in relation to Using Print Facilities. Section regarding Using Cloud Services has been added (5.9).	Head of CSD
V.3.3	27/05/2022	V3.3 – Amendments to include ICO audit (2021) recommendations	Head of CSD

Policy

Statement

All users of Merseyside Police ICT systems have a responsibility to help protect these systems. Our community and partners are entitled to expect that our ICT systems and the information held by them are secure.

We must be able to demonstrate that our information is protected from both intentional and unintentional misuse. This is necessary to maintain the confidence and trust of our community and partners and to be compliant with relevant legislation and conditions of use (e.g. Codes of practice or connection).

Aims

This policy aims to safeguard the confidentiality, integrity, and availability of our information by clearly setting out expectations regarding acceptable use of ICT systems and the devices used to get access to those systems.

The policy is underpinned by procedures designed to provide clear, definitive, and unambiguous direction for all those involved.

Objectives

A broad objective is to ensure all individuals using ICT systems, equipment, mobile devices and force information understand their personal responsibilities and are clear about what is regarded as unacceptable or inappropriate use.

More specific associated objectives are to:

a) Protect the Merseyside Police Computer Network and the information that it holds

b) Prevent disruptions to our ICT systems

c) Ensure that our ICT systems, mobile devices, and other ICT equipment are used appropriately and securely

d) Reduce the volume of security breaches

e) Protect the organisation's reputation and safeguard it from legal liabilities

f) Reinforce the professional standards of behaviour expected of all Police Officers and police staff.

g) Reduce operational risk by safeguarding confidential and sensitive information

h) Set minimum standards for use of the Internet and Email Electronic Messaging to get the maximum business benefit and eradicate unnecessary or improper use

i) Comply with the requirements of Information Management: Authorised Professional Practice

Application and Scope

This policy applies to all users who access Merseyside Police information using any Merseyside Police ICT system or device belonging to or leased by Merseyside Police.

All Police Officer, Police Staff including contractors, volunteers, agency, and temporary staff who process personal data it is mandatory that they must read the following policies and procedures upon induction and refresh re-reading them annually.

Data Protection Policy
ICT Acceptable Use Policy
Information Security Policy
Records Management Policy

Failure to comply with this policy may lead to a breach in system or information security and may lead to disciplinary action. Any suggestion that an individual is in breach of the standards required will be thoroughly investigated and they may be liable to disciplinary action. Criminal and/or disciplinary action will be taken against any user who wilfully misuses ICT systems made accessible to them by Merseyside Police.

The Chief Officer lead for this policy is the Deputy Chief Constable.

Outcome Evaluation

The Anti-Corruption Unit (ACU) and Information Assurance Coordinator (IAC) will monitor compliance with this policy.

The ACU is responsible for ensuring use of ICT systems and the processing of force information is audited and monitored. Relevant data will include the number of cases investigated by the ACU and complaints/referrals to Professional Standards Department (PSD) on associated issues.

The IAC will oversee the reporting of security breaches and monitor them.

The Information Assurance Team staff will monitor compliance with the requirement to read the policies mentioned above.