ICT Acceptable Use

POLICY (only)

OFFICAL

Government Security Classification Scheme	***Policy section:*** **OFFICIAL - Force website approved** ***Procedure section:*** **OFFICIAL-SENSITIVE**
Department of Origin	CSD Corporate Support & Development (CSD)
Policy Holder	Head of CSD
Policy Author	Information Security Officer (ISO)
Related Information	Computer Misuse Act Data Protection Act Freedom of Information Act Government Protective Marking Scheme/Government Classification Scheme Policy Official Secrets Act Police and Criminal Evidence Act Records Management Policy & Procedure Regulation of Investigatory Powers Act Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations
This Version	3.7
Created / Modified	22/06/2026
Last Approved (SMB)	25/04/2012
Review By	01/10/2027

Contents

Policy

National Context

Authorised Professional Practice (APP) is produced by the College of Policing as the official source of professional practice on policing. All officers and staff are expected to have regard to APP in discharging their responsibilities. Essentially, our "policy" is to comply with APP as it develops to cover all areas of policing.

The Information Management: Authorised Professional Practice module produced by College of Policing is the national standard we must comply with when accessing or processing information.

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 and force information understand their personal responsibility and are clear about what is regarded as unacceptable or inappropriate use.

Application and Scope

All police officers and police staff, including the extended police family and those working voluntarily or under contract to Merseyside Police must be aware of, and are required to comply with, all relevant policy and associated procedures.

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.

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

Data Protection Policy
ICT Acceptable Use Policy (this document)
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 Security Officer (ISO) 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 ISO will oversee and monitor the reporting of security breaches and compliance with the requirement to read the policies mentioned above.