# Acceptable Use Policy (Ver 5)

## 1. General Conditions

This Acceptable Use Policy (AUP) provides a summary of the main conditions of use of the Gloucestershire Constabulary (GLOS POL) Force Wide Network and is to be read in conjunction with the following Force Information Assurance Policies:

- E-mail Security Policy.
- Information Security Policy
- Government Security Classification Policy.
- Internet Security Policy.
- Network Security Policy.
- Data Protection Policy.

It is your responsibility to ensure you meet the Constabulary's policies and standards. Breaches may result in disciplinary action or criminal proceedings.

## 2. Line Management Responsibility

Line Managers are to ensure their staff follow this AUP, be proactive in ensuring compliance with it and in reporting any possible or suspected breaches to Information Security via the Breach process.

## 3. Need to Know Principle

The Need-To-Know principle mandates that knowledge of, possession of, or access to, sensitive information created/owned or held by you or vital equipment assigned to you, is to be limited to those persons who clearly have a legitimate requirement for such information and equipment in order to discharge their duties. Thus a rank or appointment held, or the possession of any level of security clearance, does not confer an automatic right of access to any information or equipment.

## 4. Malware

The Force's antivirus software (McAfee's) frequently scans all workstations including connected peripheral devices (CD/DVD & USB) for the presence of viruses and malicious code. If these are identified a warning message will be automatically displayed on your screen informing of the infection, if this message appears it is critical that you follow this message; **STOP WORKING,** contact the ICT support desk on Ext 4444 or after hours the Force Control Room Sgt on Ext 4189. Remove any CD/DVD or USB device, isolate them and wait for the IS support team to contact you.

## 5. Passwords

New users will be issued with a once only password that must be changed at first log on to the system. Thereafter users are responsible for creating their own passwords in accordance with the following password construction rules and guidance:

- Passwords must consist of 9 or more characters.
- Passwords must use at least three out of the following four character sets in any order or combination that the user can easily remember:
    1. Upper Case Letters: e.g. A, B, C,
    2. Lower Case Letters: e.g. a, b, c
    3. Numbers: e.g. 1,2, 3,
    4. Punctuation/Special: e.g. ! ?
- Automatic system prompts will require passwords to be changed every 90 days.
- Collar numbers, forenames, surnames, car numbers and birth dates must not be used.
- Six-failed log in attempts will result in automatic access denial. Temporary passwords can be obtained through the ICT Service Desk (Ext 4444) during normal working hours and the Force Control Room Inspector out of normal hours.

Passwords are unique to each user and must never be divulged to others.

A Password rest function has been provided to allow users to rest their passwords. Details on the procedure can be found on Insight.

## 6. Security of Workstations

Installation, connection to network resources and maintenance of all Force IT equipment may only be carried out by authorised Information Technology personnel. Users are prohibited from moving equipment, connecting additional equipment or installing additional software by any means.

Users must ensure workstations are locked or logged off whilst not in use.

Terminals will automatically lock out after 15 minutes inactivity.

Whilst in use, users should make sure unauthorised persons cannot view displayed data.

## 7. GSC

The GLOS POL Network is accredited to process data classified by the Government Security Classification (GSC) OFFICIAL. You must not process material higher than OFFICIAL, (which includes material marked OFFICIAL-SENSITIVE). When you create a new document you, as the originator, are responsible for deciding what its Protective Marking should be and whether any handling instructions are required. The Protective Marking and any handling instructions should be inserted as header and footer labels. All GSC material must be secured and disposed of in accordance with the GSC policy and guidance handout.

## 8. Prohibited Activity

The following activities are expressly prohibited:

- Illegal, fraudulent or malicious activities.
- Activities for the purposes of personal or commercial financial gain.
- Scanning or copying material in breach of copyright.
- Introducing software of any description without authorisation.
- Engaging in political activity.
- Authoring, transmitting or storing any data containing racist, sexist, defamatory, offensive, abusive, illegal or otherwise inappropriate material (unless needed to support an official Police investigation).
- Using another user's account.
- Attempting to avoid or defeat security measures.
- Permitting an unauthorised user to access Force systems.
- Sending information marked OFFICIAL or otherwise sensitive data via an open insecure Internet connection.

## 9. Identity

To enhance the security environment all personnel (exempt uniformed officers) must prominently display either their warrant card or identity badge at all times whilst on Force premises.

## 10. CD/DVD/USB Facilities

Users are not to import large volumes of unauthorised data onto the system. Requests for permission to have a CD/DVD writer installed or use of an authorised USB device will require the authority of a Head of Department and approval from the Force Information Security Officer (ISO).

## 11. Data Protection

Data held on Force systems may only be processed in compliance with the Force's Data Protection Registration requirements. Where any doubt exists, Users should seek the advice and guidance of the Data Protection Officer.

## 12. Reporting Security Incidents

All users have a responsibility to report actual or suspected breaches of security to the ISO either directly or via the ICT Service Desk.

An information security incident is an unexpected event that leads to the deliberate, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Constabulary information.

It could be caused by loss/theft (documents or ICT assets), insufficient control over access, equipment failure, human error, environmental causes such as fire, a hacking attack or deception.

Please report any incidents via the Security Incident/Breach Report template form which is available on inSIGHT.

## 13. Personal Use

All GLOS POL IT systems are provided for official Police purposes and not to be used to gather information for personal interest.

Accessing the internet, for personal use, from a Force workstation is not permitted.

Personally owned devices are not to be used for Official work unless authorised by Management.

## 14. Auditing and Monitoring

The Force reserves the right to monitor all such information processes to protect the confidentiality, integrity and availability of systems, ensure compliance with legal and regulatory requirements and investigate and detect security breaches and unauthorised use. Monitoring procedures are based on the principles of necessity, justification and proportionality.

## 15. Secure e-mails

The constabulary has purchased Egress which allows you to send OFFICIAL e-mails, or large files via an encrypted e-mail route. Further details are in the E-mail security policy.