



Internet Security POLICY



Policy Title – INTERNET SECURITY POLICY

Table of Contents

Introduction	1
Purpose	1
Compliance	1
Section 1 - Permitted Uses	2
Section 2 – Accessing Audio and Video Streams	2
Section 3 – Internet Filtering	2
Section 4 – Internet Monitoring	3
Section 5 - Social Networking Sites (SNS)	3
Section 6 – Staff conducting Specific Investigations	4
Section 7 - Unauthorised Access	4
Section 8 – Legal Issues	4
Section 9 – Supporting Documentation	4
Identification, Monitoring and Review	5

Introduction

It is the policy of the Chief Constable and the Office of the Police and Crime Commissioner (OPCC) for Gloucestershire to provide Internet access for authorised members of our staff. This may include temporary and contract staff where this is required for their role. The Internet access is provided for official use, i.e. for the business and administration of the Constabulary and (OPCC). Personal use of the internet is not permitted.

All Internet usage will be recorded and electronically monitored. Use of the Internet will be compliant with legislation, with regulatory obligations and with our policies.

Purpose

Whilst our connection to the Internet offers numerous potential benefits, it can also open the door to some significant risks to data and systems, if users do not follow appropriate security discipline. Users may be held accountable for any breaches of security or confidentiality resulting from their use of the Internet connection. The overriding principle is that security is everyone's responsibility.

Unnecessary or unauthorised Internet access causes network and server congestion. It slows other users, takes away from work time and consumes supplies and ties up printers and other shared resources. Unlawful Internet access may also result in negative publicity for the Constabulary or OPCC and subsequent exposure to significant legal liabilities. Therefore the purpose of this document is to state our Policy on the use of the Internet.

This policy is applicable to all personnel provided with this facility by Gloucestershire Constabulary.

Compliance

This policy has been prepared taking account of prevailing legislation. New legislative requirements or changes in current legislation may necessitate a review of this policy document.

Our policies are intended to promote equality, eliminate unlawful discrimination and actively promote good relationships regardless of: age, disability, gender, race or ethnicity, religion and Belief and sexual orientation.

This policy has been impact assessed using the Equalities Impact Assessment Template. By building equality considerations into our policy-making process, we have been able to identify any actual or potential inequalities and reduced them as much as possible, by applying the policy differently or looking for alternatives.

This policy is suitable for publication under the Freedom of Information Act 2000.

This Policy should enable consistent and effective decision making. Where operational or managerial circumstances require any decision making that would adversely affect adherence to the policy or procedure, in line with the 'Statement of Intent' of the constabulary and the police service 'Code of Ethics', if an officer/ police staff member believes that they need to make a decision that steps outside of policy and procedure they should do so, provided that:

- The officer/ police staff member raises the matter at the earliest opportunity (and ideally before any such decision is made) with their line manager declaring their intended (or actual) course of action if notification is made after the decision is taken,
- Produces, in a timely manner, a signed and dated written explanation of why it is/ was deemed necessary to step outside of policy and procedure, and
- Maintain an adequate record of this written rationale for audit purposes appropriate to the circumstances/ contravention

Section 1 - Permitted Uses

Our Internet facility is used for official use by staff in the execution of their work related functions.

If there is a business requirement for you to access the internet from a Force workstation and Force issued mobile device then you can do so.

The threat from the internet of being infected from Malware has increased so when accessing web pages you must be very cautious and suspicious, especially of the following:

- Frequent screen advertising page pop ups encouraging you to click on the link, which you must not follow.
- Advising you about new software updates, which must not be followed, this is done by ICT in a controlled way.
- Advising you that the Antivirus software has expired, click on a popup to update it, this must not be done.
- Do not download files, programs or applications without ICT approval.

If you think that you have inadvertently started downloading files or it appears that files are being downloaded then you are disconnect the internet connection and inform ICT enquires.

Any breach of the rules in this Policy could result in an investigation, disciplinary action and possible termination of employment.

Section 2 – Accessing Audio and Video Streams

It is prohibited for staff to listen to audio (radio stations) and news associated video streams (news clips & BBC iPlayer etc) via the internet from your Force workstation.

Whilst it's permitted to use these facilities for official policing purposes, personal use is prohibited.

Section 3 – Internet Filtering

Internet filtering is in place which will block the download of potentially malicious files from the internet and also block access to web sites which are known to present a security risk.

If a risky file or web site is accessed then a message will be displayed in the web browser saying that access has been denied. (A link to the warning notice).

The following file types will be blocked as standard:

All compressed files with the extension title of; 7zip, ARC, ARJ, BinHex, BZIP2, .z, CPIO, GZIP, LHA, LHARC, CAB, RAR, Stuffit, TAR, ZIP

All executable and application files with the extension title of; exe, bin, msi

All BitTorrent files with the extension title of; torrent

If you have a genuine business need to access a website or download a file which has been blocked then please email ICT.Enquiries@gloucestershire.pnn.police.uk requesting to have access or for the file to be released, with the following information:

Address of the web site:

The type of file you need to download:

Frequency of access/download required:

Business justification for the request:

Please raise the request as soon as possible to avoid any distribution which will be approval by Information Assurance. If the web site has been hacked access will not be approved but if there are no issues then permission will be given. The files will be examined for malware and if not infected released from ICT. If there is an ongoing requirement to have these files from a web page or for you to access web page then they will be added to a white list (approved list of web pages and files from appropriate web page) and should not be blocked in future.

Section 4 – Internet Monitoring

All Internet use is monitored and we reserve the right to inspect all files stored in private areas on their network and personal computers at any time, without notice, in order to assure compliance with policy.

Sexually explicit or offensive material may not be displayed, archived, stored, distributed, edited or recorded using our computer networks or resources. Any employee, who becomes connected accidentally to a site that contains sexually explicit or offensive material, must terminate the connection and log off regardless of whether that site had been previously deemed acceptable by any screening or rating program.

Employees should have no expectation of privacy when accessing the Internet through a Force account.

Section 5 - Social Networking Sites (SNS)

Social Networking Sites on the Internet such as Facebook, Bebo, MySpace and Friends Reunited are just one of many ways in which people can socialise with each other. These types of sites could potentially be accessed using our Internet browsing facilities therefore to prevent the risk of sensitive information getting into the public domain, which might bring the Police Service into disrepute, personnel are reminded they must not use official e-mail addresses to register or create blog sites.

Staff registering or accessing these sites by private means (home computers) are reminded that:

- There is a duty of confidentiality about some work issues;
- There may be personal safety issues;
- Staff must not bring discredit upon the Constabulary or OPCC.

The Force has a corporate presence, maintained and managed by Corporate Communications, on Twitter, Facebook and other SNS.

Further information on the use of SNS can be found in the Force Social Media Policy and another leaflet entitled 'Guidance to all staff from the Professional Standards Department on Social Media' which can be both found on inSIGHT.

Section 6 – Staff conducting Specific Investigations

Members of staff who need to access SNS or other sites that contain pornographic, obscene, racist or sexist material during the course of their official duties must first obtain approval from a supervising officer, which should be recorded.

Section 7 - Unauthorised Access

Users are not to attempt to access the Internet except by the route and method approved and devised by the ICT.

Section 8 – Legal Issues

Particular care must be taken to ensure the following does not occur:

- **Misrepresentation.** This can also occur unintentionally, particularly through the use of external e-mail. Employees should know, and make it clear to those with whom they communicate, that any opinions expressed are their own and not the Constabulary's or OPCC's.
- **Unauthorised contract.** Be careful not to enter into any agreement with an external agency through e-mail and the Internet. This could constitute a legal contract and prove embarrassing and expensive for the Chief Constable and Police and Crime Commissioner.
- **Data Protection.** Never disclose information about people over the Internet. There are also disclosure and security issues!
- **Libel.** Opinions expressed over the Internet and by e-mail may be recorded and could be used in litigation against the Chief Constable, Police and Crime Commissioner and/or the sender.
- **Breach of confidentiality.** An employee who reveals confidential information, including financial, strategic, technical, organisational or operational information over the Internet or by e-mail will be guilty of a breach of confidentiality and may breach the Official Secrets Act.

Section 9 – Supporting Documentation

This Policy must be read in conjunction with any specific instructions issued for each information facility and the following supporting documentation:

- Information Security Policy
- E-Mail Security Policy
- GSC Policy
- Acceptable Use Policy (AUP)
- Data Protection Policy

Identification, Monitoring and Review

Security Marking:		NOT PROTECTIVELY MARKED	
Document Title: POLICY			
INTERNET SECURITY POLICY			
Type	URN	Strategic Board	Author/Reviewer
Policy	030	IGB	Steve Davis Sara Armstrong
Version	Date	Changes (ensure public copy amended and uploaded to external website)	Complied with Policy Guidance ✓
5.2	26 Jan 17	Annual review, insertion of DCC comment, Compliance	✓
Next Document Review Date:			
EIA	EIA Sign Off		EIA Review
LOW	26 Jan 17		26 Jan 21
SIA	SIA Sign Off		SIA Review
Not required	N/A		N/A
<i>This version will be placed on the public domain website</i>			
If this version cannot be placed on the public domain website, provide reason and relevant COG authority and FOI version			