PD 140 – INTERNET & E-MAIL USE

Registered number:	PD 140
Registered Owner:	Information Security Manager
Author:	Pat Stocker
Effective Date:	July 2012
Review date:	July 2013
Replaces document (if applicable)	PD 094 E-mail Policy
Aligned to strategy:	Information Assurance Strategy
Version:	1.5
Linked Procedures/:	Open Source Research Policy Management of Standalone Computers

.

Signed: _____ Date: _____

Pat Stocker

Post: Information Security Manager

Authorised: _____ Date: _____

Det Supt Jackie Alexander

Head of Professional Standards

VERSION 1.2 DOCUMENT HISTORY

VERSION	AUTHOR	DATE	COMMENTS
1.2	Mark Weston	October 2004	First published version
1.3	Mark Weston	August 2005	Amended
1.4	Mark Weston	February 2006	Section 3 Amended – new location of G686
1.5	Pat Stocker	July 2012	Amended and incorporated e-mail policy

NOTTINGHAMSHIRE POLICE INTERNET AND E-MAIL PROCEDURES

1. BACKGROUND

1.1 This document defines the acceptable use of Nottinghamshire Police Internet and E-mail facilities and applies to all Police Officers and Police Staff, including the extended police family and those working voluntarily or under contract to Nottinghamshire Police, agency workers, contractors and third parties with access to Nottinghamshire Police's information assets.

1.2 The use of the term 'staff' within the rest of this document applies to ALL of the categories of personnel identified in 1.1 above.

1.3 The use of Internet and Email facilities via the Nottinghamshire Police network has enabled invaluable sources of information to become more widely available throughout the Force. Used for legitimate purposes, the Internet and e-mail systems can assist staff considerably in carrying out their day-to-day work. However, there are risks associated with using these facilities. These include:

- Breaches in security created by staff inadvertently or deliberately posting sensitive Force information onto Internet websites or included in e-mails;
- The introduction, to Force systems, of viruses, worms and trojans contained within downloaded files or e-mail attachments;
- Hackers accessing Force systems via Internet connections, either to steal or modify information, or to disrupt the Force's computer services and Hackers accessing Force information by intercepting those sent across the open Internet;
- The unauthorised downloading of material that is offensive, illegal or unacceptable within the workplace;
- Time wasting – either in the form of Internet surfing (casual or random browsing of Internet websites) or where websites are accessed for private rather than Force purposes or using the e-mail facilities for private purposes including as a chat mechanism with another individual either internal or external;
- Compromise of the Force's network performance by memory-intensive activities such as the downloading of large audio or graphics files;
- The downloading of software onto the Force network or onto Force standalone computers, without proper regard to copyright or licensing issues, or to potential hardware or software compatibility problems.

1.2 This policy has been developed with the aim of addressing and minimising risks associated with the Force's use of the Internet and Email facilities. In order to do this, the policy specifies acceptable use of these facilities by all Force staff in all circumstances and consideration is given to Internet and Email related disciplinary issues associated with deliberate or negligent breaches of this or other Force policies.

PART ONE – INTERNET USE

2. GENERAL CONDITIONS OF INTERNET USE

2.1 The conditions in this section apply to all Internet use within the Force, irrespective of the device used:

- Access to the Internet via Force computers is provided for business use only. **Private use is strictly forbidden;**
- Staff must not submit sensitive Force information, including protectively marked material, to any website
- Other than their own personal details, staff must not submit personal information to any website without the written consent of the individual(s) to whom the information relates, or, where this is not possible, without the authority of a representative from the Force Data Protection Team;
- No attempt must be made to use the Internet in any way that breaches UK legislation;
- Staff must not download or use copyrighted information contained on websites other than in compliance with the copyright conditions;
- No deliberate attempt must be made to use the Internet in any way that might disadvantage the Force or bring the Force into disrepute;
- Staff must not, under any circumstances, create websites that purport to represent the Force or any part of the Force;
- No material may be placed onto the Force website, other than via the Corporate Communications Department and in compliance with any relevant Force policy;
- Under no circumstances may any member of staff allow his or her Internet facilities to be used by any other individual.
- No attempt must be made to access any website that is of a disreputable, criminal or of a recreational nature under any circumstances.
- The downloading of any computer software onto the Force network from an Internet website must be referred to the Information Services Department via a Service Desk call, they are then responsible for virus-checking the software, ensuring that it is legitimate and ascertain that its use complies with any copyright and licensing conditions. The Information Services Department must also establish that the downloaded software will not conflict with system hardware or other software already in use within the same system. If these conditions are satisfied, the software must, before use, be recorded on the Information Services Software Asset Register

2.2 INTERNET ACCESS VIA THE FORCE NETWORK – GRANTING ACCESS

2.2.1 Access to the Internet will be available to all Nottinghamshire Police Force LAN account holders. This will allow access to most websites that are now a day-to-day requirement for most Police Officers, Staff and other Nottinghamshire Police LAN account users in fulfilment of their duties.

Sites that remain blocked on networked machines fall into the following categories:

- Pornography / Adult Content - *Sites that portray sexual acts and activity.*

- Gambling Sites *which encourage gambling such as betting sites, bookmaker odds*
- Adware Sites *that promote or offer software that collects information about users*
- Bad Reputation *Sites that appear on one or more security industry blacklists for repeated bad behaviour*
- BotNet Sites *used by botnet herders for command and control of infected machines*
- Hacking information *revealing the ability to gain access to software or hardware/communications equipment and/or passwords*
- Phishing - *Deceptive information pharming sites that used to acquire personal information for fraud or theft*
- Freeware/Shareware Sites *that provide repositories of shareware and freeware for download*
- Games Sites *related to computer or other games, such as game download sites, online games*
- Chat Sites *offering chatrooms and chat services*
- Malicious Code Sites *that promote, carry malicious executable, or worm code that intentionally causes harm*
- Peer to Peer / File Sharing Patterns *which block the use of peer-to-peer file sharing network*
- Remote Access Sites *provide information about or facilitate access to information, programs, online services or computer systems remotely*
- Spyware Sites *that promote, offer or secretively install software to monitor user behaviour, track personal information*,
- WebMail Sites *that offer online web based e-mail services; this excludes ISPs, which provide standard POP or IMAP e-mail accounts*.

2.2.2 Access to specifically blocked sites may be allowed for a limited period following a request to Service Desk. The Information Security Team will make a decision on a case-by-case basis. Use of the Service Desk portal for requests is mandatory to ensure that a record is maintained of who has been provided with access and why it is required. This process means that for future upgrades of the filtering software, Information Services hold the correct information to ensure authorised users retain their required access levels.

2.2.3 Please note that if you require greater access to social networking sites for investigation purposes you should refer to the Open Source Research Policy or contact the Covert Authorities Bureau.

2.3 INTERNET ACCESS FROM STANDALONE COMPUTERS, - PLEASE REFER TO THE ‘MANAGEMENT OF STANDALONE COMPUTERS POLICY’

2.3.1 Internet access from any standalone computer must only be available where the required type of access would be inappropriate from the Force network and in conjunction with the Management of Standalone Computers policy.

2.4 FORCE POLICY ON THE MONITORING OF INTERNET ACTIVITY

2.4.1 Internet activities of individuals via Force systems is not subject to real time monitoring but extensive logs of all Internet activity are maintained within the system. From time to time these logs will be used to produce a wide range of usage statistics. In addition, filtering software is in place to help ensure that Internet use complies with Force policies. Where the reports from this software identify a potential policy breach, a representative from Information Security determines the appropriate response. A physical examination of an individual's Internet activity will only be made in these circumstances, or where it is necessary in order to investigate suspected breaches in legislation, of this policy or of other Force policies.

2.4.2 A regular audit regime is also in place for the purpose of identifying officers and staff that feature as the top users of the Force internet system through an on-going audit process. Reports are sent out quarterly to relevant Heads of Department and Divisional Commanders, where members of staff within their Department/BCU have been identified in the list of top users. Relevant managers are then responsible for confirming that these users have a legitimate police business purpose for using the Internet to that extent.

2.5 CONSEQUENCES OF INTERNET ABUSE

2.5.1 Any Internet use that breaches this policy or other Force policies will potentially attract disciplinary action. Where it is established that an individual's misuse of the Internet may also have involved a breach in legislation, a criminal investigation that may lead to prosecution will always be considered.

2.5.2 When considering disciplinary action, line managers must take the following issues into account:

- Whether the individual who committed the breach reported it at the earliest opportunity.
- The extent to which the breach may have occurred deliberately, through negligence or by accident. It is quite possible, for example, for an individual to access a disreputable website inadvertently, particularly where a hyperlink, the website's address or a description of its content provides a misleading impression of its true nature. In order to help establish this, the individual concerned should be required to describe his or her work-related actions that led to the breach. It may be necessary for the line manager to obtain audit logs of the individual's Internet activity in order to confirm or refute the explanation given. Consideration should also be given to how many occurrences of a particular type of breach have taken place involving the same individual or group of colleagues. Several similar breaches, particularly over an extended period of time, may require more explanation that a single breach.
- The severity of the incident. As with other types of disciplinary issue, the line manager will be required to exercise his or her judgement in this respect.
- In addition to establishing any action that may need to be taken against an individual as the result of a breach, the line manager must also consider if it is appropriate to remove or limit the individual's Internet access level.
- Where any doubt exists regarding appropriate action, the Professional Standards Department should be contacted for advice.
- Where it is suspected that an individual's use of Force Internet facilities breaches legislation, the Professional Standards Department must be contacted immediately.

- If a suspected breach is likely to require the involvement of the Professional Standards Department, and the suspected breach involved a stand-alone or laptop PC, the machine should be taken out of service immediately and stored securely in order to preserve any evidential material that may be contained on the machine.

PART TWO – EMAIL USE

3. GENERAL CONDITIONS OF EMAIL USE

3.1 The Force e-mail service is provided for a police business purpose only and must not be used for private purposes. **The use of either internal or external Force e-mail facilities for the following purposes is strictly forbidden**:

- Private or freelance business. This includes transacting the sale of personal goods.
- Betting
- Importing, receiving and transmitting pornographic, obscene or sexually exploitative material onto the Force network under any circumstances.
- Importing, receiving and transmitting pornographic, obscene or sexually exploitative material onto standalone Force systems unless this forms part of a properly authorised investigation.
- Transmitting of offensive, obscene and abusive messages and images, or other material that is of a defamatory, harassing or bullying nature.
- Any act of discrimination, contrary to legislation or Force policies or that is offensive to the dignity of people at work.
- Conducting political activities.
- Participating in electronic chain mails. Any electronic chain mails received must be deleted immediately and NOT passed on under any circumstances.- if unsolicited please see the reference to SPAM below.
- Unsolicited e-mail received must be forwarded to the internal ‘SPAM’ mailbox for processing and deleted from individual or shared mailboxes.
- Deliberate or negligent disclosure of Force information to unauthorised persons.
- Deliberate or negligent introduction of malicious software onto the Force network under any circumstances.
- Deliberate or negligent introduction of malicious software onto any Force system, other than the Force network, unless this forms part of a properly authorised and controlled investigation.
- Deliberate or negligent introduction of any material infringing copyright law onto any Force computer.
- Using e-mail to breach any other Force policy.

3.2 Use Of Force E-Mail Facilities For Semi-Official Matters

Force e-mail facilities may be used to publicise or communicate information relating to the following semi-official activities:

- Officially sanctioned charities.
- Non-profit making sports and social events.
- Non-commercial offers of, or requests for help or assistance.
- All of the above categories may now be placed on the Force Intranet within the 'Social' arena i.e. Market Place, Noticeboard, Charity Work and Sports News. For further information please contact the Force Internal Communication Team.

3.3 Use of Public Folders

The Force has a number of public folders, which are variously used to provide all staff, or large groups of staff, with information. It is important that each of these folders is used only for its designated purpose.

3.4 Conditions of Use of Force External E-Mail Facilities

3.4.1 The external transmission of any e-mail using Force facilities must comply with the following conditions:

- External e-mails that relate to official Force business must only be sent from devices that are connected to the Force network.
- The sensitivity of each e-mail's content must be established in accordance with the Government Protective Marking Scheme, assigning, where relevant, a protective marking. The relevant protective marking must be identified in some part of the e-mail, this may be within the body of the e-mail, identified in the subject header or added as a generic statement within the electronic signature.
- A document whose sensitivity equates to a protective marking of RESTRICTED must not be e-mailed to any external e-mail address, unless the address is contained in the list below (see 3.5). These addresses indicate that the e-mail will be transmitted over the Criminal Justice Extranet (CJX) or the Government Secure Internet (GSI), both of which systems provide a greater degree of security than that of the Open Internet. An example of a RESTRICTED document is something containing personal data, which may cause a risk to an individual's safety or liberty, hinder the detection or impede the investigation of low level crime or cause the prosecution of such crime to collapse, cause an undermining of confidence in public services or reputational damage to the Force if compromised.
- A document whose sensitivity equates to a GPMS protective marking of CONFIDENTIAL or above must not be e-mailed either internally or externally using the standard Force network. A separate CONFIDENTIAL E-MAIL SYSTEM is available via the Force Confidential Network for use with the Police National Database (PND). Guidance on this system is available on the PND site of the Force Intranet. For further advice please contact the Information Security Team.
- The e-mail must be correctly addressed, with particular consideration given to the potential impact if that e-mail should go astray.
- Staff should also be aware of the auto function in outlook, which tries to auto-complete the recipient line for you and if not checked may send the e-mail to an incorrect destination.

- It is recommended that staff do not bulk load large amounts of personal data into one e-mail. The data should be separated in order to reduce the risk and the overall impact if the e-mail were to be compromised.

- The sender of an external e-mail must ensure that its content does not commit the Force to any contractual obligation, unless the sender is authorised to do so.

- Every external e-mail must include the relevant Force disclaimer (see below), which is automatically added to the bottom of any e-mail.

Unless otherwise stated please treat as restricted

Internet e-mail is not to be treated as a secure means of communication. Nottinghamshire Police monitors all Internet e-mail activity and content. This communication is intended for the addressee(s) only. Please notify the sender if received in error. Unauthorised use or disclosure of the content may be unlawful. There is no intent, by Nottinghamshire Police, that this e-mail should constitute a legally binding document, nor do opinions expressed herein necessarily represent official policy.

Find out about Nottinghamshire Police by visiting www.nottinghamshire.police.uk

- Nottinghamshire Police is not responsible for the content of any E-mail and cannot guarantee that a message will remain private, confidential or free from legal consideration.

- Nottinghamshire Police retains the right to monitor, intercept and disclose the content of any E-mails sent or received, all of which are the property of Nottinghamshire Police.

3.5 List of secure e-mail addresses

3.5.1 Secure email domains in Central Government:
*.gsi.gov.uk
*.gse.gov.uk
*.gsx.gov.uk

3.5.2 The Police National Network/Criminal Justice Services secure email domains:
*.police.uk
*.pnn.police.uk
*.scn.gov.uk
*.cjsm.net

3.5.3 Secure email domains in Local Government/Social Services:
*.gcsx.gov.uk

3.5.4 Secure email domains in National Health Service:
*.nhs.net.uk

3.6 Abuse of E-Mail

3.6.1 Any abuse or suspected abuse of e-mail must be reported in the first instance to the

appropriate line supervisor, who will instigate any necessary remedial and disciplinary action. Where virus infection is suspected, the Service Desk must be contacted immediately for advice or assistance. No attempt should be made to transmit any file that is suspected of containing a virus, even as part of an internal investigation, unless Information Services have advised that it is safe to do so.

3.6.2 The Force Information Security Team must be advised of any abuse or suspected abuse of e-mail at the earliest opportunity. Where necessary, line management will liaise with the Information Security team to progress the matter. Deliberate failure to report identified abuse of the e-mail will be considered as condoning that abuse and may, itself, be the subject of disciplinary action.

3.6.3 Where any offence or misconduct involving e-mail use is suspected, accounts will be accessed by authorised individuals only, without necessarily notifying the individual who is under investigation. Any evidence revealed will be presented to the relevant Force disciplinary body.

3.6.4 Conducting any of the activities forbidden under this policy constitutes misconduct and may result in appropriate disciplinary action being taken. Where it has been established that an individual has used e-mail to breach another Force policy, disciplinary action that is appropriate to that policy will be taken. Where it is discovered or suspected that an individual's email use breaches legislation, prosecution may be considered.

3.6.5 Generally, any item found on the system which is in breach of the e-mail policy will be removed from the system by Information Services following receipt of authority from the investigating officer, at the first possible opportunity. The mailbox user and their supervisor will then be advised. Occasions may arise when infringing articles are left on the system during the progress of an investigation. This will only occur where to delete the item(s) would compromise the investigation. On these occasions, deletion will then be authorised by the investigating officer at the appropriate time.

3.7 Responsibilities

3.7.1 All staff must recognise that if they fail to abide by the e-mail policy, they will be held personally liable for their own actions. The Force will always investigate and take action where necessary, to protect the interests of the Force and its employees. Such investigations will be conducted in compliance with Human Rights and other relevant legislation or guidance.

3.7.2 The usual Force policy relating to confidentiality of passwords giving access to Force systems applies to all e-mail. Users must not let other people use their personal e-mail box.

3.7.3 Individuals remain responsible for the items dispatched or contained in their e-mail accounts at all times. The only exception to this is where an individual receives an unsolicited item that breaches the policy, and where that recipient reports this breach at the earliest opportunity. The onward transmission or retention of offending items that has been authorised by a supervisor, for the purpose of investigating an abuse, will not itself constitute a breach of policy.

3.8 Access and Maintenance of Mailboxes

3.8.1 Where a mailbox is assigned to an individual, he or she is responsible for its maintenance. Due to the following circumstances under which the content of e-mails may be checked, individual users should not assume that the content of any e-mail that they send or receive, using a Force system, will remain private.

3.8.2 Filtering software is used to ensure that the content of e-mails sent from and received by the Force complies with Force policies. Where these measures identify that an email may have breached Force policy, the Information Security Team will determine how that e-mail should be dealt with. This may involve a designated individual checking the content of the e-mail where it is felt necessary to do so.

3.8.3 Access to an individual's mailbox without gaining his or her permission will only be made in the following circumstances and following a formal request to the Service desk portal:

- When a request for access to another persons Outlook account whilst they away from work for an extended period is received, the customer requesting access must specify what access they need and the reason why. Requests must be received from the relevant line manager or a senior manager within the Department. Direct Requests will not be accepted from colleagues. The Information Security Team will then assess each request on a case-by-case basis and authorise the relevant access levels via Information Services and an out of office message placed on the account.

3.9 Further Guidance

- To contribute to the efficient flow of e-mail traffic throughout the Force, users should avoid sending excessively large e-mails, particularly where this is to a large number of recipients.
- Keep it short, professionally worded and to the point.
- To assist the recipient, make the title meaningful to the content.
- Check your e-mail account regularly - at least once a day where possible.
- Use the 'Out of Office Assistant' (found under Outlook's Tools) to indicate when you are out of the office, when you will return, where you can be contacted (if applicable) or where e-mails should be re-directed and other relevant contact details.
- Before sending an e-mail with attachments, ensure all addressees have the ability to open any attachment.
- To reduce the electronic size of e-mails, logos and pictures should be removed wherever possible, before an e-mail is sent.

LEGISLATIVE COMPLIANCE STATEMENT

This document has been drafted to comply with the general and specific duties in the Equality Act 2010; Data Protection Act; Freedom of Information Act; European Convention on Human Rights; Employment Act 2002; Employment Relations Act 1999, and other legislation relevant to policing.