Making Northern Ireland Safer For Everyone Through Professional, Progressive Policing

FREEDOM OF INFORMATION REQUEST

Request Number: F-2009-03353

Keyword: Complaints/Discipline

Subject: COMPUTER MISUSE SINCE JANUARY 2005

Request and Answer:

Question 1
The date of the alleged offence and the date it was settled / dealt with.

Question 2
The nature of the alleged misuse - e.g. excessive internet usage, looking at inappropriate material, use of social networking websites, installing forbidden software etc.

Question 3
The position held by the employee - officer rank or department if a police civilian.

Question 4
Was the case upheld and details of any disciplinary action taken.

Question 5
A copy of the report if one was produced (please redact names in accordance with Data Protection laws).

Answer
Professional Standards Department within the Police Service of Northern Ireland is responsible for internal discipline and therefore holds data in relation to Police Officers. Information reported to the PSNI's Professional Standards Department is not recorded centrally and would have to be extracted from an interrogation of their electronic databases. Due to the nature and way this information is held a check of up to 5 categories would be required in order to identify appropriate investigations. Once these appropriate files have been identified each file would have to be examined manually in order to extract specific information requested. It has been estimated that this retrieval would take in excess of 46hrs therefore exceeding the "appropriate limit" of 18hrs.

Information that has not been reported to Professional Standards Department in regard to Police Officers but may have been investigated and dealt with by local management is not held centrally; similarly Civilian Staff that may have been reported for such disciplinary offences are investigated and dealt with by Local Management or Human Resources Management. This information is not held centrally either. In order to retrieve the information on both Police Officers and Civilian Staff has been estimated to take in excess of 64hrs therefore further exceeding the "appropriate limit" of 18hrs.

I would like to draw your attention to the fact that there is no standardised way to collate the requested information within different Districts which is why some Human Resource Managers may be able to retrieve the information and provide a response within the time permitted under FOI legislation and other managers of larger districts would have to carry out prolonged manual searches of Personnel Records e.g. Headquarters Department Manager has a responsibility for over 2000 staff and a minimum of 20 minutes per file would take in excess of the time permitted to locate and provide the information as set down in FOI legislation.

Due to the factors above the cost of complying with your request for information in respect of questions 1 to 5 would exceed the "appropriate limit" as stated in the Freedom of Information Regulations 2004, which is currently set by the Secretary of State at £450. To provide a response to these questions would entail the extensive utilisation of resources cost well in excess of the "appropriate limit" of £450 laid down by the Secretary of State.

Further to your clarification dated 27th October 2009 the PSNI have also considered whether we can refine your request as you have suggested to bring it within the appropriate limit but unfortunately the nature and structure of this information makes this impossible.

Question 6
Also, please can you provide me with a copy of guidelines about the use of the internet given to staff, if such a document exists.

Answer
Please find document below.

If you have any queries regarding your request or this decision please do not hesitate to contact me on 028 9070 0164. When contacting the Freedom of Information Team, please quote the reference number listed at the beginning of this email.

If you are dissatisfied in any way with the handling of your request, you have the right to request a review. You should do this as soon as possible or in any case within two months of the date of issue of this letter. In the event that you require a review to be undertaken, you can do so by writing to the Head of Freedom of Information, PSNI Headquarters, 65 Knock Road, Belfast, BT5 6LE or by emailing foi@psni.pnn.police.uk

If following an internal review, carried out by an independent decision maker, you were to remain dissatisfied in any way with the handling of the request you may make a complaint, under Section 50 of the Freedom of Information Act, to the Information Commissioner's Office and ask that they investigate whether the PSNI has complied with the terms of the Freedom of Information Act. You can write to the Information Commissioner at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. In most circumstances the Information Commissioner will not investigate a complaint unless an internal review procedure has been carried out, however the Commissioner has the option to investigate the matter at his discretion.

Please be advised that PSNI replies under Freedom of Information may be released into the public domain via our website @ http://www.psni.police.uk/

Personal details in respect of your request have, where applicable, been removed to protect confidentiality.

Police Service of Northern Ireland

Acceptable Use Policy (AUP)
Information and Communication Facilities

Executive Summary

The purpose of this Acceptable Use Policy is to ensure that all users understand the way the 'Information and Communication Facilities' should be used within the PSNI. This covers the use of the Internet, Extranet, PoliceNet and E-mail facilities. The policy applies to all police and civilian staff in Departments, Regions, District Command Units and Branches, and others, including temporary / agency staff / consultants. The procedures and constraints set out in this policy are intended to protect the interests of the PSNI and users, and to ensure that individuals do not place themselves at risk of disciplinary action, criminal proceedings or civil action as a result of misunderstanding or lack of guidance.

Use of the 'Information and Communication Facilities' by PSNI users is only permitted for official purposes. They may only be used in a manner that is consistent with PSNI policing priorities, and as part of the normal execution of a user's role and responsibilities. The use of the 'Information and Communication Facilities' for any private purpose is not permitted.

Failure to comply with the contents of this policy may lead to advice or written warning from a District Commander or Head of Branch; disciplinary action, criminal or civil proceedings. In addition, should the conduct and actions of the user be unlawful or illegal, the employee / user may be held personally liable through criminal or civil proceedings.

All information relating to the operation of the PSNI is private. Users are reminded of the requirement to treat electronic information with the same care as paper-based information. All information will be kept secure and should be used only for the purpose(s) intended. The information should not be disclosed to any unauthorised person.

This Acceptable Use Policy will be updated as required.

Index

19. Definitions

1. Introduction

1.1. All electronic communication including, but not exclusively, the PSNI telephone and data network, Internet / Extranet / PoliceNet and external (Internet) / internal electronic mail are collectively known as our 'Information and Communication Facilities'. 'External (Internet) / internal electronic mail' are known as our E-mail facilities.

1.2. Access to 'Information and Communication Facilities' will be available to police and civilian support staff (users) within the Police Service of Northern Ireland (PSNI) when the 'Common Terminal' roll out is complete. Such access will enhance the overall operational effectiveness and efficiency of the PSNI.

1.3. It must be clearly understood that 'Information and Communication Facilities' are provided for PSNI business use only, and not for private use. As such; all electronic communications and documents, are the property of the PSNI. The PSNI will audit all such media: automatically by computer software, and manually. Therefore privacy of use cannot be assumed.

1.4. Anyone who uses the 'Information and Communication Facilities' within their role and responsibilities, and complies with this AUP, has nothing to worry about. Anyone who abuses the 'Information and Communication Facilities' will be subject to further investigation.

2. Purpose

2.1. The purpose of this policy is to ensure that all users understand the way the 'Information and Communication Facilities' should be used within the PSNI. The procedures and constraints set out in this policy are intended to protect the interests of the PSNI and users, and to ensure that individuals do not place themselves at risk of disciplinary action, criminal proceedings or civil action as a result of misunderstanding or lack of guidance.

2.2. Failure to comply with the contents of this policy may lead to advice or written warning from a District Commander or Head of Branch; disciplinary action, criminal or civil proceedings. In addition, should the conduct and actions of the user be unlawful or illegal, the employee / user may be held personally liable through criminal civil or proceedings.

3. Scope

3.1. This document outlines the Acceptable Use Policy (AUP) of the PSNI in relation to all users of 'Information and Communication Facilities'. The policy applies to all police and civilian staff in Departments, Regions, District Command Units and Branches, and others, including temporary / agency staff / consultants.

4. General Principles

4.1. Use of the 'Information and Communication Facilities' by PSNI users is only permitted for official purposes, for example, to contact other police forces, to research relevant police related issues, to assist with ongoing criminal investigations or to send E-mail to bona fide addresses. They may only be used in a manner that is consistent with PSNI policing priorities, and as part of the normal execution of a user's role and responsibilities. The use of the 'Information and Communication Facilities' for any private purpose is not permitted.

4.2. The use of PSNI 'Information and Communication Facilities' are subject to European / UK / NI law and the PSNI Code of Ethics and relevant Civil Service instructions. Any inappropriate use will be investigated.

4.3. Users of our 'Information and Communication Facilities' will at all times conduct themselves honestly, accurately and appropriately. Users must comply with: software licensing rules; property rights, copyrights, and respect the privacy and prerogatives of others. Current PSNI policies relating to personal conduct apply to the users of the 'Information and Communication Facilities'. If abuse of the facilities is suspected, line managers should take appropriate steps in accordance with normal disciplinary procedures under paragraphs 901 - 1100; and disciplinary procedures from Para 1060 to 1096 of the NICS manual in the case of civilian staff or the Code of Ethics in respect of police staff. (Or the Code of Conduct/1988 Discipline Regulations if the use was prior to the publication of the Code of Ethics.) All users and supervisors can seek further advice and guidance from the Superintendent ICS.

4.4. Users should note that they could be personally liable to prosecution and open to claims for damages from aggrieved individuals, if their actions are found to be in breach of the law. In this context, all police personnel and civilian support staff should note that the absence of an intention to harass is not a defence. If someone sees material they consider offensive – perhaps simply by walking past a screen and inadvertently seeing text or an image displayed – they may claim that they have been subjected to harassment. In such cases, all individuals involved in the chain of events leading to a complaint may be liable to legal action and / or disciplinary action, even if they had no intention of the material being seen by others. Police Supervisors shall also have regard to Article 10.2 of the Code of Ethics.

4.5. Impersonation of another system user (i.e. logging on using their password) opens the way to behaviour equivalent to "poison pen" letter writing. There is a clear onus on all users to keep their password secret. For example: passwords must not be written on post it notes and stuck to the monitor, under the keyboard, etc. The log on process to the common terminal will alert users to the last time they logged on, and also alert them to any failed attempts to log on (i.e. user name or password incorrect). If any password abuse is suspected,

users and line managers should take appropriate steps in accordance with the normal disciplinary procedures under paragraphs 901 - 1100; and disciplinary procedures from Para 1060 to 1096 of the NICS manual in the case of civilian staff, or the Code of Ethics in respect of police staff (Or the Code of Conduct/1988 Disciplinary Regulations). All users and supervisors can seek further advice and guidance from the Superintendent ICS.

4.6. Users may delegate others to handle and manage their E-Mail, calendar, etc. on their behalf. This is to be encouraged to ensure that important messages are not overlooked when a user is off duty, unavailable, on leave, etc. This means that other users know that an approved delegate is responding, and there is no attempt to assume any other person's users name and password.

4.7. As part of the common terminal roll out, training is provided. Users should familiarise themselves on how to use the Outlook 'Out of Office' assistant; how to set up delegates (to which your E-Mail will be forwarded while you are out of the office.) This is most important when a user is on leave or on a course.

5. Internet

5.1. The Internet is a vast network that electronically connects millions of people worldwide. The World Wide Web, (www) also called 'the Web': presents information via the Internet using a 'browser' that includes multimedia formats such as; graphics, sound, animation and video.

5.2. The Internet is a superb resource, especially for research purposes. However it is very insecure. Once on the Internet, users should be aware that your movements, (i.e. what sites you visit) and what you type or send (i.e. E-Mail) can be captured by unscrupulous people. Such people set up programs that capture everything you type, and attempt to recover passwords or any information that they can use for their own purposes. Their activities are mainly concerned with attempting to get information that can help them gain access to networks, so that they can search around. However if they came across any 'juicy' E-Mail, it may find its way to a tabloid newspaper, in a similar way to people record conversations on the mobile telephone network. Users therefore must be most careful when browsing the Internet and using Internet E-mail. All invitations to download a required file or plug-in, must be treated as suspect. All users and supervisors can seek further advice and guidance from the Superintendent ICS.

5.3. Our Internet access is protected by a substantial firewall. This firewall protects all users from viruses and programs that may attack the integrity of our systems. It automatically prevents dangerous files being received or downloaded from the Internet. Normal Internet connections do not provide this service; which is why all Internet access must be through the official Internet connections, and any attempt to use alternative Internet connection is strictly prohibited. The firewall is designed to protect the PSNI network. It will not protect users from unscrupulous people exploiting the information that users share once they are on the Internet. All users and supervisors can seek further advice and guidance from the Superintendent ICS.

5.4. Access to the Internet will be based on specific roles and responsibilities within Departments, Regions and District Command Units. Authorisation will be to a named individual, according to their role and responsibilities.

5.5. Users will **not**: upload; download, use, retain, distribute or disseminate any images, text, materials or software which:

- 5.5.1. Are or might be considered to be indecent, obscene, pornographic or illegal (for exemptions refer to Section 7, sexually explicit and offensive material);
- 5.5.2. Are or might be offensive or abusive in that its context is or could be considered to be a personal attack, inappropriate, or unjustifiably and personally critical, sexist, racist, or generally distasteful;
- 5.5.3. Involve activities outside the users role and responsibilities, for example, private use; might be defamatory or incur liability on the part of the PSNI or adversely impact on the image of the PSNI;
- 5.5.4. Would be a breach of copyright or license provision with respect to either programs and data, and
- 5.5.5. The user cannot, or is not, prepared to account for.

5.6. Users will **not**:

- 5.6.1. Send or forward any material that is intended to annoy, harass or intimidate another person;
- 5.6.2. Make or post indecent remarks, proposals or materials on the Internet;
- 5.6.3. Use the Internet to perform online transactions, for example, banking, shopping etc., unless authorised as part of their official duties;
- 5.6.4. Use the Internet to play games;
- 5.6.5. Download non-business related software or data including music, graphics, videos, text, games, entertainment or pirated software;
- 5.6.6. Participate in chat rooms, forums or newsgroups unless this is for official purposes within the users role and responsibilities, and has been approved by a supervisor.
- 5.6.7. Remain connected to the Internet while they are not actively using the resource. An Internet connection should not remain 'live' when it is not actively being used (e.g. for convenience).

5.7. A user who innocently receives, or connects, to any Internet site that contains inappropriate, sexually explicit or offensive material will disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program. The user will report the matter to their supervisor immediately, who will submit a report to the Superintendent, ICS Lisnasharragh outlining the

details of the incident. Supervisors must encourage staff to comply with this direction, because the material, once viewed, will have already been logged and saved under that users name. Any user who innocently receives such material by connecting to a site in these circumstances, will want to ensure that any audit will not suggest that they have been viewing inappropriate material. Superintendent ICS will ensure, that in such circumstances, the offending material is properly deleted and records perfected accordingly. All users and supervisors can seek further advice and guidance from the Superintendent ICS.

5.8. While our firewall protects us internally from malicious external users on the Internet, users are reminded that the Internet is inherently insecure. Therefore, users must not divulge any information that may be regarded as confidential or sensitive in nature. This relates not only to Internet E-mail, and E-mail attachments (that may contain personal information) but also to the completion of online forms. Again, users and supervisors can seek further advice and guidance from the Superintendent ICS.

6. Connecting devices to the Network.

6.1. All laptop computers, other than those officially issued by ICS, are strictly prohibited from accessing the Internet via PSNI telephone lines. Officially issued laptops may only have access to the Internet following approval by Superintendent ICS, and only official dial up connections to carefully selected and approved service providers are permitted. Therefore, connecting to unapproved service providers such as FreeServe, AOL, etc., from an official laptop is **not** permitted. Section 5 above outlines why.

6.2. Laptop computers or any other device may **not** be connected to the PSNI network.

6.2.1. All devices (personal or issue) that have at any time been connected to the Internet (or may be connected to the Internet at some future time) must not be connected to the network.

6.2.2. This includes PDA's, SmartPhones, Mobile phones, USB disk drives, USB pen drives, etc.

6.3. All devices, e.g. PDA's, SmartPhones, Mobile phones, USB disk drives, USB pen drives, etc., (whether Internet capable or not) will not be connected to any 'Information and Communication Facilities' or the PSNI telephone lines unless there is prior approval from the Superintendent ICS.

6.4. USB connectivity to 'Information and Communication Facilities' will only be permitted if a case has been made and approved. In such cases the USB port will only accept the approved device, and any attempt to connect anything else will be recorded as a security threat and will be subject to investigation.

7. Sexually Explicit and / or Offensive Material

7.1. In accordance with this policy: users will not; upload, download, use, retain, distribute or disseminate any images, text, materials or software which are or might be considered to be indecent, obscene, pornographic or illegal.

7.2. Police officers investigating crimes involving material of a sexual or offensive nature may, subject to the approval of the Senior Investigating Officer (SIO), access / download such material that may assist with the investigation. Police investigating other crime that, by reason of the criminal culture, is linked with pornography (e.g. piracy, copyright theft, computer security) should seek approval of their SIO who must consult with the Superintendent ICS.

8. Extranet

8.1. An Extranet is a collection of networks or Intranets that are linked as a 'closed community', that provides an internal E-mail facility and access content on Extranet web, and other information servers in a secure environment.

8.2. The Criminal Justice Extranet (CJX), of which the PSNI is an integral member, is a managed network that is operated on behalf of the Police Information Technology Organisation (PITO).

8.3. This Extranet fulfils two primary objectives, providing:

8.3.1. A single, standardised interconnection of police forces and other Criminal Justice Organisations (CJO's), and

8.3.2. A common connection point to the Internet for organisations connected to the Extranet.

8.4. The CJX Extranet will permit users to send documents marked Restricted or lower when the network has received formal accreditation. Under no circumstances will users send protectively marked documents of Top Secret, Secret and Confidential level via this E-mail system. The PSNI sensitivity labels are:

8.4.1. Confidential - PSNI;

8.4.2. Restricted - PSNI;

8.4.3. Restricted - PNN; and

8.4.4. Unclassified - All Networks.

9. PoliceNet

9.1. PoliceNet is the PSNI PoliceNet, which is simply an information resource held on PSNI computers that communicate with each other and provide an internal E-mail facility. Its contents will reflect, corporate information, local information, and other reference material.

9.2. Accordingly: the PoliceNet provides access to information electronically; such as General Orders, Code Regulations, Finance Regulations, Service Policies and Reports, Service wide briefings and initiatives, Government Initiatives, and the Internal Telephone Directory.

9.3. Users will not upload, download, use, retain, distribute or disseminate any images, text, materials or software which:

9.3.1. Are or might be considered to be indecent, obscene, pornographic or illegal (for exemptions refer to Section 7, sexually explicit and offensive material);

9.3.2. Are or might be offensive or abusive in that its context is or could be considered to be inappropriate, or unjustifiably and personally critical, sexist, racist, or generally distasteful;

9.3.3. Involve activities outside the scope of responsibilities, for example, unauthorised selling/advertising of goods and services;

9.3.4. Might be defamatory or incur liability on the part of the PSNI or adversely impact on the image of the PSNI;

9.3.5. Would be a breach of copyright or licence provision with respect to either programs or data, and

9.3.6. The user cannot or is not prepared to account for.

9.4. Users will not:

9.4.1. Send or receive any material that is intended to annoy, harass or intimidate another person;

9.4.2. Make or post indecent remarks, proposals or materials on the PoliceNet;

9.4.3. Use the PoliceNet to play games;

9.4.4. Participate in chat rooms, forums or newsgroups unless this is for official purposes.

10. Editorial Content on the PSNI Internet / Extranet / PoliceNet Sites

10.1. All electronic publication is controlled and approved by the Director of Information Management, who has responsibility for all E Publishing.

10.2. Internet

10.2.1. Users will not upload, update or amend any information on to the PSNI Web site without express approval of the PSNI Webmaster. Where there is a requirement to upload, update or amend such information details should be forwarded to the PSNI Webmaster, who will consult with the Director of Information Management as required.

10.3. PoliceNet

10.3.1. Editorial content of the PSNI PoliceNet site is the responsibility of E Publications, Lisnasharragh. Users will not upload, update or amend any information on to PoliceNet without express prior approval of the E Publications. Where there is a requirement to upload, update or amend such information details should be forwarded to E Publications, who will consult with the Director of Information Management as required.

10.4. Neither of the above are intended to preclude staff (specifically District Commanders or their equivalent in HQ Branches or Departments) from preparing, designing or suggesting inclusions on the Internet/Extranet/PoliceNet, but are intended to ensure a professional corporate approach, and to minimise any potential technical difficulties. Users can seek further advice and guidance from the PSNI Webmaster, E Publications or the Superintendent ICS. (Essentially a Word document will suffice.)

11. Electronic Mail (E-mail)

11.1. When writing E-mail, users will ensure that the message meets the standards of professionalism and integrity required by the PSNI. PSNI Code of Ethics and NICS Manual apply. Users will not make any statements on their own behalf or on behalf of the PSNI; which do, or may, defame, libel or damage the reputation of any person or the PSNI.

11.2. Care should be taken when using E-mail because E-mail messages are perceived to be less formal than paper-based communication, and there is a tendency to be lax about their content. It should be borne in mind that all expressions of fact, intention and opinion via E-mail can be held against the user and / or the PSNI in the same way as verbal and written expressions.

11.3. Be aware that phrases that are normally exchanged face to face, person to person, may not be fully understood in an E-mail message. A user reading E-mail will not have the advantage of seeing the person face to face, and therefore sarcasm and comments intended to be humorous may not be received or interpreted as such.

11.4. Any E-mail sent using another users ID and password will be considered as fraudulent.

11.5. Users will not use E-mail facilities to:

11.5.1. Engage in any activity that is illegal, distasteful or likely to have an adverse impact on the PSNI;

11.5.2. Forge or attempt to read other users' mail without their express permission;

11.5.3. Use the E-mail facilities to send or forward anything that is not business related; this includes PowerPoint files, video files and greetings cards that are not clearly business related. Such E-mails and their attachments would be a serious breach of our network capacity.

11.5.4. Promote or participate in any chain mail. Chain mail has the potential to overload the network and can cause distress or offence to those who receive it;

11.5.5. Forward, send or store E-mails or other files containing inappropriate materials, and

11.5.6. Use E-mail facilities in any way, which is not within the normal execution of their roles and responsibilities, unless expressly permitted by a supervisor.

11.6. Internal E-Mail

11.6.1. Users will make themselves aware of the protective marking scheme as it applies to documents, be they electronic or hard copy.

11.6.2. In order to minimise congestion on the PSNI network, file attachments for uploading on the Internet will be restricted to 4MB using the Microsoft Office and Adobe Acrobat applications. When an attachment exceeds this limit, the sender will be advised of the failed delivery and should make alternative arrangements accordingly. Users should be aware that the use of graphics and other images in e-mails and their attachments consume large volumes of network capacity and therefore the use of colour representations of the PSNI crest, etc., on internal communications is to be discouraged.

11.7. . **External or Internet E-mail**

11.7.1. Internet E-mail is insecure, and therefore nothing of a confidential or sensitive nature should be sent.

11.7.2. Access to all E-mail Internet sites (e.g. Hotmail, Yahoo mail etc.) is restricted due to the potential threat of viruses being spread and infecting the network. The use of Internet E-mail for private use is not allowed.

11.7.3. The contents of all E-mail will be automatically scrutinised in order to ensure that all communications comply with the provisions of this policy.

12. Working from home

12.1. The PSNI has devoted considerable resources to update our 'Information and Communication Facilities'. Users cannot copy files to the Internet or any device to be recalled from a home system. To do so would be a breach of the Data Protection Act.

12.2. Clearly there is a need to help dedicated staff to allow them to work out of the office. The Director of Information Management and ICS are working on a solution that will not breach the Data Protection Act.

13. Protective Markings

13.1. HM Government has established 5 categories of Protective Marking and these categories will apply to similarly classified documents within the PSNI. The 5 categories are as follows:

13.1.1. Top Secret

13.1.2. Secret

13.1.3. Confidential

13.1.4. Restricted

13.1.5. Not Protectively marked.

13.2. Only documents marked Confidential or lower may be sent via the internal E-mail system. Under no circumstances will users send protectively marked documents of Top Secret, Secret level via the internal E-mail system.

13.3. The PSNI sensitivity labels are:

13.3.1. Confidential - PSNI;

13.3.2. Restricted - PSNI;

13.3.3. Restricted - PNN; and

13.3.4. Unclassified - All Networks.

13.4. For security reasons only those documents graded 'not protectively marked' should be sent on the external E-mail system. The sending of all other classified documents is strictly prohibited. Therefore Internet E-mail cannot be used for anything that could be interpreted as sensitive. Section 5 and 11 above refer.

13.5. It will be the responsibility of the sender to ensure that the proper classification is afforded and due diligence is applied. Those who contravene this direction may be subject to disciplinary action.

13.6. For advice and guidance on the appropriate classification of documents users should refer to the PSNI Service Information Security Policy – SISP 1/2001, dated November 2001, and where applicable appropriate training should be sought and acquired. All users and supervisors can seek further advice and guidance from the Superintendent ICS.

14. Training

14.1. The roll out of the common terminal includes training for all staff. This training will include this AUP.

14.2. Anyone who feels that they require training, or additional training, should consult their local personnel officer.

15. Address Convention

15.1. In accordance with ACPO guidelines on police E-mail, the appropriate address convention will be:

15.1.1. personal-identifier@forcename.pnn.police.uk

15.2. Accordingly a user's address will read as follows:

15.2.1. john.smith@psni.pnn.police.uk

15.3. In the event of there being more than one John Smith within the PSNI, the address will read:

15.3.1. john.smith@psni.pnn.police.uk,
15.3.2. john.smith2@psni.pnn.police.uk and so on.

16. Confidentiality

16.1. All information relating to the operation of the PSNI is private. Users are reminded of the requirement to treat electronic information with the same care as paper-based information. All information will be kept secure and should be used only for the purpose(s) intended. The information should not be disclosed to any unauthorised person.
16.2. Users must return any message received that was intended for another recipient and will delete any copies of misdirected messages. An incorrectly addressed message should only be forwarded to the intended recipient if the identity of that recipient is known and certain.
16.3. Users will verify that the recipients of the E-mail are approved to receive the information contained in the E-mail, to avoid a breach of confidence. All users and supervisors can seek further advice and guidance from the Superintendent ICS.

17. Security

17.1. The Information System Security Policy provides full advice, guidance and directions. This section of the AUP outlines a summary of the main areas as they affect the 'Information and Communication Facilities'.
17.2. 'Firewalls' have been established in order to ensure the safety and security of the PSNI networks. Any user who attempts to disable, defeat or circumvent these will be subject to investigation and appropriate disciplinary action.
17.3. Users will not:
17.3.1. Use the 'Information and Communication Facilities' to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of the system, network or another user;
17.3.2. Examine, change, or use another employee's files, output, or user name for which they do not have explicit authorisation. Passwords remain confidential and the sharing of passwords/IDs is prohibited;
17.3.3. Use the 'Information and Communication Facilities' to propagate any virus, worm, trojan horse, trap-door program code, password capture program, or;
17.3.4. Seek to gain access to restricted areas of the network outside the authorised user profile.
17.4. Internet E- mail is the most prolific source of computer viruses, which can cause considerable disruption to our network. The PSNI Firewall protects us, however any E-mail, or any files taken from a laptop or other device that has been connected to the Internet are a most serious threat. See Section 5 above. Immediately any user suspects that the computer they are using has a virus, the following action must be taken by the user:
17.4.1. Report the incident immediately to the Help Desk, Telephone 55555, the Help Desk will alert the Information Technology Security Officer (ITSO);
17.4.2. Respond to any advice or alerts given by the ITSO, and;
17.4.3. Report the matter in writing (not by E-Mail from the computer with the suspected virus!), via the District Commander / Head of Branch, for the attention of the ITSO.

18. Monitoring and Expectation of Privacy Issues

18.1. The Lawful Business Practice Regulations 2000 requires employers to inform staff that interceptions (even of private communications) might take place. 'General Order 54/2002 D(d) 'Monitoring of Communications' refers.'
18.2. All police personnel and civilian support staff should be aware that the PSNI has systems and software in place that can monitor and record all 'Information and Communication Facilities' to ensure compliance with security and other rules, and to ensure operational effectiveness as is permitted by legislation. It follows from this that users of 'Information and Communication Facilities' - should be aware, and must accept as a condition of use, that their usage of such facilities will be subjected to monitoring. All communications will be automatically scanned.
18.3. In addition, use will be routinely monitored from time to time, and may be specifically monitored at any time when this is deemed necessary for compliance or other reasons, including the prevention or detection of inappropriate or illegal activities. Users should not, therefore, have any expectation of privacy in relation to their use of 'Information and Communication Facilities'. The PSNI may publish usage patterns in order to ensure that 'Information and Communication Facilities' are devoted to supporting the highest levels of work productivity and the achievement of corporate objectives..
18.4. The PSNI security systems are capable of: recording and auditing (for each and every user) each World Wide Web (www) site visit; E-mail message and file transfer into and out of the network. Logs of all traffic will be monitored and archived by the Superintendent ICS.
18.5. E-mail messages that have been deleted from the system can be traced and retrieved. All E-mail messages will be archived.

18.6. Software and files downloaded via 'Information and Communication Facilities' will remain the property of the PSNI, unless proved otherwise. Copyright and software rights of any file downloaded outside this Acceptable Use Policy will clearly remain with the authors.

18.7. The PSNI reserves the right to audit and inspect any files that are stored in any area of the network in order to ensure compliance with this policy.

19. Definitions

19.1. **'Information and Communication Facilities'** includes all electronic communication including, but not exclusively, the PSNI telephone and data network, Internet / Extranet / PoliceNet and external (Internet) / internal electronic mail are collectively known as our 'Information and Communication Facilities'.

19.2. **'E-mail facilities'** includes all E-mail whether they are Internet, Extranet, PoliceNet, or Internal E-mail.

19.3. **Inappropriate material** may be simply defined as any material that may be perceived as inappropriate in the circumstances. Clearly this includes anything of a pornographic, racist, sectarian, violent or offensive nature. Examples include depictions (whether in pictures, cartoons, words, sounds or moving images) of sexual activities, violence, torture, bestiality, cruelty, humiliation and exploitation. Users should note that:

19.3.1. This list is not exhaustive,

19.3.2. It is a criminal offence to make or distribute pornography, or to have child pornography,

19.3.3. Material purporting to be of a humorous nature (including cartoons) may be deemed inappropriate, and,

19.3.4. In addition to any disciplinary penalty imposed (which could extend to dismissal) they could be open to legal action by an aggrieved party and could be held personally liable for damages awarded against them.

19.4. **Audit or Traffic monitoring** may be defined as recording and analysing websites visited, the address E-mails are sent to etc., the equivalent of recording the duration and destination of telephone calls.

19.5. **Audit, Content Monitoring**, may be defined as looking at the actual content of E-mails, files, etc., the equivalent of recording and listening to the content of telephone calls.

19.6. **Viruses**, these are programs that are designed to create havoc to any host computer. There are many different types: but all are designed to either damage the users computer files or threaten the security of our network. Our official Internet connection is protected by a firewall to protect us from such viruses. Worm, trojan horse, trap-door program code, password capture program, are all types of virus.

19.7. **Firewall**, is an intelligent barrier that prevents unauthorised access to computer systems.

19.8. **Browser**, is a program – normally Microsoft Internet Explorer - that is used to view the Internet, Extranet, or PoliceNet.

19.9. **E-mail**, is short for electronic mail. It uses a program – normally Microsoft Outlook – that sends and receives E-mail messages.

19.10. **PDA,** is a Personal Digital Assistant. Official PDA's are only issued to senior staff.

19.11. **IS**, stands for Information Systems.

19.12. **IT**, stands for Information Technology.

19.13. **Chain mail;** refers to any message that encourages the recipient, in any way, to forward the message to other users.

19.14. **Devices,** include anything that can be connected to 'Information and Communication Facilities'. It includes: USB Disk Drives, USB pen drives, all memory storage devices (including compact flash, secure digital, memory sticks), scanners, printers, PDA's, mobile phones, smartphones, laptop computers.

19.15. **USB:** Universal Serial Bus, is a way of connecting devices to a computer.

Explanatory notes:
(This section is provided to assist trainers, supervisors and users with the interpretation of the AUP).

PSNI will offer full support to the users of 'Information and Communication Facilities', if they are directly related to individuals' role and responsibilities, and there is no breach of our Code of Ethics. If there are any difficulties, concerns or problems these should be referred to the Superintendent ICS, who will help.

PSNI will <u>not</u> support any attempt to use these facilities for private use, outside the individuals' role and responsibilities, or breach of our Code of Ethics. Any attempt to use or circumvent official systems, in any way, will be drawn to the attention of the Superintendent ICS, - who will investigate. Depending on the circumstances; the details may be passed to the District Commander, Head of Branch, Internal Investigation Branch (or Human Resources Discipline) for further investigation, which may result in criminal charges or disciplinary action.

The reason why all devices are prohibited from connecting to our network is simply security. We cannot allow devices to link into our 'Information and Communication Facilities' that may at any time have been previously, or may in future be connected to the Internet. This includes linking the device with any other device that may have been, or will be,

connected to the Internet. (Section 5.2 refers) If you have any questions about this, or any other aspect of the policy please contact Superintendent ICS, telephone 21927, O7801 738344.