

**NOT PROTECTIVELY MARKED**



**EXTERNAL E-MAIL AND  
INTERNET ACCESS –  
ACCEPTABLE USE**

**FORCE REFERENCE DOCUMENT**

FRD Reference Number	I15
Quality Auditor	Corporate Services
First Issued	14.3.03
Last Updated	1.7.04
Version	3

**NOT PROTECTIVELY MARKED**

# NOT PROTECTIVELY MARKED

## POLICY

1. Northern Constabulary actively supports the Modernising Government Agenda by providing desktop access for staff to appropriate electronic communication where required. Part of this provision is extending access from within the Force to external organisations.
2. This Force Reference Document is intended to define the permitted access to the Internet and to the CJX (Criminal Justice Extranet) network.
3. Failure to adhere to this Force Reference Document may be regarded as a breach of the Police (Conduct) (Scotland) Regulations 1996, or lead to disciplinary proceedings for support staff. It may also constitute a breach of the Computer Misuse Act (1990) or the Data Protection Act (1998) and render police or support staff liable to criminal prosecution.
4. This document has been reviewed in terms of the principles of the Human Rights Act 1998 and is considered to be compliant.
5. Articles 9 and 10 of the Human Rights Act 1998 gives everyone the right to freedom of thought and expression, which includes the right to receive and impart information and ideas without interference by a public authority. Northern Constabulary seeks to protect the rights of individuals but will interfere with these rights to achieve compliance with this policy. This is necessary, proportional and transparent. To meet this aim, Northern Constabulary will use the least intrusive option available in the prevailing circumstances.

## STANDARDS

### 1. INTERNET ACCEPTABLE USE

- 1.1 The Criminal Justice Extranet (CJX) has been established nationally as a secure (up to RESTRICTED level) network forming a means for Criminal Justice agencies to communicate among themselves. The CJX connection also provides users with a connection outside this restricted network to the Internet.
- 1.2 Access to the Internet, via the CJX, is provided to assist staff in carrying out duties consistent with their responsibilities. Internet access is for business use only and may be revoked if abused. The user is personally responsible for his/her actions in accessing and utilising the Force computer resources.

NOT PROTECTIVELY MARKED

## **NOT PROTECTIVELY MARKED**

- 1.3 One important aspect of the Internet is that no one party owns or controls it. This fact accounts for much of the Internet's openness and value, but it also places a high premium on the judgement and responsibility of those who use the Internet, both in the information they acquire and in the information they disseminate to others. When subscribers obtain information through the Internet, they must keep in mind that the Force Information Security Officer cannot monitor, verify, warrant, or vouch for the accuracy and quality of the information that subscribers may acquire. For this reason, the subscriber must exercise his or her best judgement in relying on information obtained from the Internet and also should be aware that some material posted to the Internet is sexually explicit or otherwise offensive. Sites accessed by users will be logged and audited. For this reason, any person accidentally accessing a site that may be considered unacceptable should inform his/her supervisor. The incident should be logged on Form AD/18/31 by the supervisor and signed by both parties to indemnify against breach of this policy.

## **2. RISKS**

- 2.1 The connection of Police systems to any public network carries with it increased security threats. To counteract such risks, there must be adequate access controls in place to ensure the integrity, availability, and confidentiality of all Police systems.
- 2.2 The main risks to the systems at Northern Constabulary are:
  - (a) Breach of Confidentiality

The unauthorised sharing of information, whether accidental or deliberate, with a third party.
  - (b) Denial of Service

Result of an event, usually deliberate, whereby network traffic is increased to such an extent that normal use of the systems is not possible.
  - (c) Loss of Integrity

The result of an attack on systems may compromise information, leaving it in an inaccurate form.
  - (d) Unauthorised Access

Whereby a person gains access to some system by masquerading as another user, or by other illegal means.

**NOT PROTECTIVELY MARKED**

# NOT PROTECTIVELY MARKED

## 3. GENERAL INTERNET USE

Users have a unique ID that appears in transaction logs and audit trails. Users are held responsible for the transactions recorded with their ID.

The following activities are deemed unacceptable and are therefore prohibited:

### 3.1 **Intellectual Property Violations**

Engaging in any activity that infringes or misappropriates the intellectual property rights of others, including copyrights, trademarks, service marks, trade secrets, software piracy and patents held by individuals, corporations, or other entities. Engaging in activity that violates privacy, publicity, or other personal rights of others.

### 3.2 **Obscene Speech or Materials**

Using the Force network or the CJX network to advertise, transmit, store, post, display, or otherwise make available rude, indecent, sexually or racially explicit or offensive material.

### 3.3 **Defamatory or Abusive Language**

Using the Force network or the CJX network as a means to transmit or post defamatory, harassing, abusive, or threatening language.

### 3.4 **Forging of Headers**

Forging or misrepresenting message headers, whether in whole or in part, to mask the originator of the message.

### 3.5 **Unauthorised Network Access**

Activities that disrupt the use of or interfere with the ability of others to effectively use the network or any connected network, system, service, or equipment.

### 3.6 **“Spamming”**

Sending unsolicited bulk and/or commercial messages over the Internet.

### 3.7 **Facilitating a Violation of this Policy**

Advertising, transmitting, or otherwise making available any software, program, product, or service that is designed to violate this policy, which includes the facilitation of the means to spam, initiation of pinging (network discovery and mapping), flooding, mailbombing, denial of service attacks, and piracy of software.

NOT PROTECTIVELY MARKED

## **NOT PROTECTIVELY MARKED**

### **3.8 Illegal or Unauthorised Access to Other Computers or Networks**

Accessing illegally, or without authorisation, computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as "hacking"). Also, any activity that might be used as a precursor to an attempted system penetration (i.e. port scan, stealth scan, or other information gathering activity).

### **3.9 Contractual Agreement**

Any form of contractual agreement which the user does not have the authority to enter into.

### **3.10 Illegal Activities**

Engaging in activities that are determined to be illegal.

### **3.11 Other Activities**

Engaging in activities, whether lawful or unlawful, that Northern Constabulary determines to be harmful to its staff, operations, network, reputation, goodwill, or customer relations.

## **4. EXTERNAL E-MAIL CONDITIONS OF USE**

4.1 Care should be taken when using E-Mail. This medium is perceived as less formal than paper-based communications and there is a tendency to be more lax about content. Users can be held liable for all expressions of fact, intention and opinion contained in the E-Mail in the same way as for verbal or written comment.

4.2 Transmission of protectively marked information must be in accordance with the Manual of the Protective Marking Scheme. For advice on this, please contact the Information Security Officer or check the Force Information Security Policy.

4.3 If a user receives an E-Mail message for which s/he is not the intended recipient, the sender should be notified and the message deleted.

4.4 Use of large messages or attachments can have a deleterious effect on the performance of systems. Therefore, a limit on the total size of attachments to a single mail message will be imposed. Currently this stands at 10 MB (megabytes).

4.5 An E-Mail message should not contain material that can be perceived to be:

- (a) indecent or obscene;

**NOT PROTECTIVELY MARKED**

## NOT PROTECTIVELY MARKED

- (b) offensive or abusive, a personal attack, rude, sexually or racially explicit;
- (c) encouraging or promoting activities that would, if conducted, be illegal;
- (d) activities outside the scope of one's responsibilities;
- (e) adversely affecting the performance of Force networks or systems;
- (f) defamatory or incur liability on the part of the Force, or adversely impact upon the image of the Force;
- (g) likely to breach the rights of individuals;
- (h) any form of contractual agreement which the author does not have the authority to enter into.

### 5. MONITORING

- 5.1 The Force will, as necessary, log, monitor and audit any communications sent or received, Internet sites visited and files downloaded. E-Mails or attachments may be blocked automatically if certain criteria are met.

## GUIDANCE

1. The following basic guidelines are intended to help you comply with the Force

### E-Mail and Internet Policy:

- (a) Do not use a computer to harm other people or their work.
  - (b) Do not damage the computer or the network in any way.
  - (c) Do not interfere with the operation of the network by installing illegal software, shareware, or freeware.
  - (d) Do not violate copyright laws.
  - (e) Do not view, send, or display offensive messages or pictures.
  - (f) Do not share your password with another person.
  - (g) Do not waste limited resources such as disk space or printing capacity.
  - (h) Do not trespass in another's folders, work, or files.
  - (i) Do notify a supervisor immediately if, by accident, you encounter materials, which violate the appropriate use policy (see below).
  - (j) **BE PREPARED** to be held accountable for your actions and for the loss of privileges if the standards set out in this policy are violated.
2. Do not write in an E-Mail what you would not put in a letter or say face-to-face.
3. Examine business processes to see if they are unnecessarily dependent on E-Mail. E-Mail is not always the most efficient method, i.e. given the shared folders on the COE, there is often no need to attach internal documents.

NOT PROTECTIVELY MARKED