



Classification

NOT PROTECTIVELY
MARKED

TITLE INTERNET/E-MAIL PROTOCOLS
CCMT Sponsor ACC CORPORATE DEVELOPMENT
Department/Area ICT GROUP – CORPORATE DEVELOPMENT
Section/Sector

1.0 Rational

Internet access is available to all Thames Valley Police staff via desktop LAN terminals. A policy on access and usage of this facility is required.

2.0 Intention

The intention of the policy is to give clarity to staff as to how and when they can access and make use of the Internet facility. In particular, the policy offers guidance to line managers who will supervise the use of this facility.

3.0 General Principles

3.1 Accessing the Internet

Access to the Internet is allowed via the following methods:

- via the TVP mail system on the LAN
- via a TVP desktop browser approved by the ICT Department
- via a non-TVP approved Internet service provider (ISP) on a stand-alone desktop or portable PC, on the understanding that non-TVP ISPs are not supported by the ICT Department.

3.2 Using the Internet

Access to the Internet is allowed on the condition that it is being used by staff as an appropriate business tool. (e.g. for research or information relating to the individual's role.) However, personal use is also permitted in a member of staff's own time (i.e. meal breaks; before or after work begins) providing that, in the line manager's view, such usage does not affect the user's performance in his/her day-to-day role, and on the understanding that the user conforms with the Force internet policy at all times.

Instructions for users who have Internet access on their desktops or via stand-alone PCs are as follows:

- users must not access the internet when logged in as a user other than themselves
- each user is responsible for the internet activity that takes place while they are logged in
- users must take care not to leave their machine unattended without the screensaver password activated
- users do not use the facility inappropriately, as outlined in 4.3.

3.3 Inappropriate use of the Internet

Internet facilities must not be used to:

- Compromise the name and/or the reputation of TVP
- Make unauthorised financial commitments of TVP
- Represent personal views as those of TVP
- Intentionally retrieve or disseminate unsuitable or confidential material
- Distribute or receive unauthorised copyright materials
- Conduct a personal business enterprise
- Send chain letters
- Conduct political activity and/or fund-raising
- Make harassing or offensive statements, (including any debasement of race, sex, national origin, sexuality, age, disability, religious or political beliefs)
- Knowingly take any action which would expose TVP to viruses
- Any action which is unlawful
- Design or build a site in the name of TVP

E-mail should not be automatically forwarded to an address outside the TVP network if the intended recipient is out of the office. This is because correspondents may send a document marked "restricted" or higher not knowing how you have set up your mailbox, and consequently this document could be passed to an unsecured network. The responsibility for this would be with the receiver, not the sender

The above are guidelines and not intended to as a comprehensive list. It will be a matter for line managers to determine whether an individual's usage is inappropriate with regard to all the circumstances.

3.4 Use of Laptops and Personal Computers Outside TVP Premises

All of the rules and recommendations in this document apply equally to TVP equipment residing outside TVP premises. This equipment is the personal responsibility of the staff member to whom it was issued. If it is lost or stolen this must be reported by the user to the police, their line manager and ICT Customer Services.

4.0 Decision Making Process

Consequences of inappropriate or improper usage

- 4.1 If a line manager suspects that a member of staff is using the Internet inappropriately the manager can request a spot check from the ICT Department. This request must be forwarded to ICT Customer Services. The result of the audit will be reported back to the line manager in question, who would be responsible for raising with Human Resources any issues that might result in disciplinary or other action being taken, in line with existing policies. All such investigations will be in strict confidence, in order to protect staff whatever the results may be. If any security issue is involved ICT Customer Services will also bring the matter to the attention of the Force Data Protection and Information Security Officer.
- 4.2 Where an individual is found to have abused their access to the internet, either through inappropriate or improper use (e.g. excessive non-work related access during working hours, or any of the points detailed in 3.3 above) then that individual may be liable to any or several of a number of sanctions. These range from withdrawal of Internet access to more formal disciplinary procedures as already specified within TVP personnel policies. The sending of offensive or sexually explicit messages or images will, in most circumstances, constitute gross misconduct which could lead to dismissal

5.0 Challenges/ Representations

Challenges and representations relating to this policy should be made in writing and addressed to:

Head of ICT Group
Thames Valley Police Headquarters
Oxford Road
Kidlington
Oxon
OX5 2NX

APPENDICES**General Rules, Recommendations, and Advice****E-Mail**

1. E-mail distribution lists should be used responsibly. Global and Directory level e-mail distribution lists should only be used for TVP business or officially sanctioned events. Group and Team level lists may be used at the discretion of the relevant managers. All User e-mails must receive prior official authorisation from Corporate Information.
2. E-mail is primarily for use in the course of your duties. Occasional and reasonable personal use is however acceptable.
3. Internet e-mail is not secure. You should not send any information that is classified as "restricted" or higher via Internet e-mail
4. When on duty/at work, you should endeavour to access your e-mail at least once a day.
5. You should not send large attachments in e-mail. Place them in an open file where the intended reader can access them. If you need advice over this procedure, contact ICT Customer Services.
6. Ask yourself whether you would be happy for your e-mail to be read out in court.
7. Avoid making libellous or derogatory comments in e-mail.
8. Please be aware that all e-mail is stored for a certain amount of time and can in principle be read, although it is not TVP policy to do so as a matter of course.(see *Lawful Business Monitoring Policy*).
9. While the mail system will automatically add a disclaimer to e-mail, if you feel there is any possible ambiguity as to whether an e-mail you are sending is on your own behalf or on behalf of TVP, include a statement clarifying which is the case.
10. It is recommended that you keep hard copies of e-mails with substantive content, or keep archived copies somewhere off the network, e.g. on floppy, or zip disc.
11. It is illegal to send via e-mail anything that it is illegal to possess in the first place.
12. Harassment and discrimination are just as illegal electronically as they are in the "real" world.
13. Remember that e-mail content is subject to the Data Protection Act 1998 and subject access provisions.
14. Do not open any e-mail attachment if you do not know what it is.
15. Try to avoid copying e-mails to people who do not need them

16. If you receive e-mail purporting to contain a warning about computer viruses, inform ICT Customer Services and do not open it
17. Ignore junk e-mail. If junk e-mail from the same source persists, contact ICT Customer Services.
18. Always remember that e-mail does not have a guaranteed delivery time. If your message needs to be received in five minutes, e-mail may not be the best medium for it.
19. If the file you wish to attach is stored in a public folder, consider sending a link to it instead of sending the actual file. If an attachment is necessary, include a sentence saying what it is in the body of the e-mail. Recipients should not have to guess what it is you have sent them. Attachments to be sent outside TVP should be saved in Rich Text Format where possible, as you cannot be sure that the recipient will be using Microsoft Word.

Web Access

20. Any message that passes through the Internet gateway uses bandwidth on the TVP network. High volumes of traffic could potentially affect the service provided to all users. In the normal course of events, one user could not provoke such a load on the system with two possible exceptions;
 - Downloading of large files from the Internet. Please use common sense as to the timing of this, or use a standalone machine. If in doubt consult ICT Customer Services.
 - Usenet news groups, mailing lists, and “push” channels. These can be subscribed to and provoke a large volume of traffic. While it is accepted that there may be cases where such subscriptions could be useful for the fulfilment of work duties, it is recommended that this use be confirmed with line management. ICT Group Customer Services should be informed so that ICT Group staff is aware of the reasons for the volume of traffic.
21. Do not deliberately visit, view, or download any material from any Web site containing illegal material or material which others might reasonably consider offensive.
22. Do not download executable software without consulting with your manager and with ICT Customer Services. In any event, any executable software not specially authorised to run will fail. Your manager should confirm that it is needed and ICT Customer Services should confirm that such a download would not place an unacceptable load on the network. Such software should then be run on a standalone machine, or portable.
23. Be aware that there is such a thing as copyright law, and the fact that it is easy to break does not mean it should be broken.

Security Software

24. Security software monitors and, on occasion, prevents some usage of the Internet and electronic mail. Its presence is required to ensure the best possible protection and integrity of the TVP network and equipment. Amongst its functions are:
- Virus detection of file transfers.
 - Blocking of ActiveX and/or Java code. These are programs, which automatically load to your PC from web pages and then run themselves.
 - Protection against loss of confidential information from cookies or via 'spyware'. A cookie is a file created on your PC at the request of a web page to store information. Web pages can call these files back and read them. While most have an innocent purpose, this technique is open to abuse by unscrupulous web designers. "Spyware" is a catch-all term referring to programs planted inside web-browsers, which send information back to web-servers without the user's knowledge.
 - Searches for offensive keywords or phrases on Web pages
 - Blocking of undesirable sites. **See below**
 - Filtering of undesirable file types.
 - Blocking of junk mail.

If you suspect or find that the Force security measures are actually preventing you from carrying out your duties you should contact ICT Customer Services (700-6700).

25. Force policy is to block access to particular sites and particular categories of sites. The primary intention of this is to protect the reputation of Thames Valley Police and the security of the TVP network. The list of prohibited sites is maintained by the supplier of our web content security software. False positives are still possible and access blocked unnecessarily should be reported to ICT Customer Services.
26. Standalone PCs with Internet access are not subject to any of the automatic restrictions but staff using them are still subject to the Internet access policy.

No security software provides or guarantees total safety. The presence of this software does not mean that staff are absolved from using their common sense when using the Internet. This applies particularly to files of unknown provenance.

Categories of Sites to which access will be blocked

27. *Adult Content*
Sites featuring full or partial nudity reflecting or establishing a sexually oriented context, but not sexual activity; sexual paraphernalia; erotica and other literature featuring, or discussions of, sexual matters falling short of pornographic; sex-orientated businesses such as clubs, night-clubs, escort services, password/verification sites. Includes sites supporting online purchase of such goods and services.

28. *Sex*
Sites depicting or graphically describing sexual acts or activity, including exhibitionism.
29. *MP3*
MP3 sites are websites either containing pre-recorded music mp3 files or that serve as directories of such sites. These files can be downloaded onto your computer. **99% of MP3 downloads may be violating copyright.**
30. *Gambling*
Sites that provide information about or promote gambling or that support online gambling. Risk of losing money possible.
31. *Games*
Sites that provide information about or promote electronic games, video games, computer games, role-playing games, or online games; also sites that support or host online games. Includes sweepstakes and give-aways.
32. *Illegal/Questionable*
Sites that provide instruction in, or promote, crime or unethical or dishonest behaviour or evasion of prosecution thereof.
33. *Hacking*
Sites providing information on or promoting illegal or questionable access to or use of communications equipment and/or software.
34. *Internet Communications*
Web chat. Sites that host Web Chat services, Chat sites via HTTP, on-IRC chat rooms. Home pages devoted to IRC. Sites that offer forums or discussion groups.
35. *Racism/Hate*
Sites that promote the identification of racial groups, the denigration or subjection of groups (racially identified or otherwise), or the superiority of any group.
36. *Internet Auction*
Sites that support the offering and purchasing of goods between individuals.
37. *Tasteless*
Sites that cannot be categorised elsewhere but offer offensive, grotesque, frightening, lurid material with no redeeming value.
38. *Violence*
Sites that provide information on or promote violent activity. Sites containing excessive profanity may be classified here if not under Tasteless.
39. *Weapons*
Sites that provide information on, promote, or support the sale of weapons and related items.

While it is unlikely that any of the above will result in the blocking of access to sites needed for work related activity that possibility does exist. Requests for exceptions to any restrictions should be submitted to ICT Customer Services for onward consideration.

Human Rights Certification

a1. Legal Basis

Data Protection Act 1998 including rights of subject access
Computer Misuse Act

ACPO Community Information Security Policy

Government Protective Marking Scheme

Telecommunications (Lawful Business Practice) Interception of Communications
Regulations 2000

a2. Human Rights Articles Engaged

It is acknowledged that this policy has the potential to engage the following Articles:

- Article 8 The Right to Respect for Private and Family Life

In the event that an Article of the Convention is engaged, the legitimacy for the engagement is provided within the text of the Article:

Article 8 The Right to Respect for Private and Family Life - necessary in a democratic society, for the protection of public safety, for the prevention of crime and disorder, for the protection of the morals of others, for the protection of the rights and freedoms of others.

- Article 10 – Freedom of Expression

In the event that an Article of the Convention is engaged, the legitimacy for the engagement is provided within the text of the Article:

Article 10 Freedom of Expression – the exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions, or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of health or morals, for the protection of the rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of judiciary.

a3. Prohibition of Discrimination

By engaging any of the aforementioned Articles, there is the potential to engage Article 14 of the Convention. The enjoyments of the Rights and Freedoms set forth in the European Convention of Human Rights shall be secured without discrimination on any grounds, such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with national minority, property, birth or other status. Actions taken as a consequence of this policy will be applied fairly and impartially, having due regard for natural justice and human rights.

<u>CHECKLIST</u>

a4. Health and Safety at Work

This document does not have Health & Safety implications. However, care should be taken to ensure compliance with Health & Safety (Display screen Equipment) Regulations 1992 and regular workstation assessments should be carried out (ref.: Workstation Assessment form on the LAN).

a5. Data Protection/Freedom of Information/Disclosure

This policy reflects the legal obligations and responsibilities outlined within legislation governing the above issues and it has been formulated after detailed consultation with the Force Information Security Officer and the Data Protection Officer.

a6. Best Value Implications

The implementation of desktop Internet access will have a number of results. It will allow for more efficient working practices in that staff will not have to move to a separate terminal and will make a useful resource readily available to all staff. It will result in a reduction of the number of individual ISP accounts currently held by areas and departments, and will result also in a reduction of the number of standalone machines currently in use. It is anticipated that a number of these standalone terminals will be converted to network machines.

This policy has links with the Best Value Review of ICT within the Best Value 5 year Review Programme

a7. Extent of Consultation

The draft protocols have been circulated to the Staff Associations, Force Solicitor, Head of Human Resources, Force Information Security Officer, Head of Corporate Information, Force Internal Communication Manager, ICT SG members, ICT Heads, ICT Technical staff. The Policy Advisory Group agreed the principles contained within this policy on 9th April 2002. The Chief Constable's Management Team agreed this policy on 12th June 2002.

Publication**a8. Links to Police National Legal Database/Other Policies**

E-mail Policy, Lawful Business Monitoring Policy, Information Systems Security Policy

a9. Communication Strategy

This policy will be published on the Force Intranet prior to the implementation of Internet access for all users. The existence of the policy will be publicised in Force Weekly orders and via an all user e-mail. It is also recommended that the policy is included in the induction packs of all staff.

a10. Target audience

The protocols contained in this document are intended for Thames Valley Police personnel and those attached to Thames Valley Police, including temporary, casual and volunteer staff.

a11. Public Availability

This policy can be made available to the public.

a12. Protective Markings

The policy is to be classified as “Not Protectively Marked”

Review

a13. Review Process

This policy will be reviewed every two years.

The review process will take into account the following:

- Changes in domestic and European legislation
- Changes as a result of Home Office circulars/ACPO guidelines/Audit Commission/HMIC
- Results of National, European and Strasbourg Court rulings (i.e.: case law)
- Complaints received as a result of a policy (in conjunction with Professional Standards)
- Representations made by relevant bodies or persons (e.g.: Local Government, members of the public)