



<u>Policy Title</u>	Electronic Communications
<u>CCMT Sponsor</u>	Director of Information, Science and Technology
<u>Department/Area</u>	Corporate Communications Department
<u>Section/Sector</u>	ICT

---

### **1.0 Rationale**

This policy covers the use of all Force electronic communication systems both internal and external which are provided for business purposes. These include the intranet, internet and e-mail, and any process that uses these systems as an operating platform such as blogs, Facebook, YouTube or Twitter. Authorised users must, at all times, comply with this policy and the accompanying Force Electronic Communications Standards, for each method of communication i.e. E-mail, Internet, Intranet and Social Networking.

### **2.0 Intention**

The intention of this policy is to give staff and managers clear guidance on the use, and supervision of users, of these systems. The policy applies equally to users of Force approved terminals as well as other electronic devices inside and outside TVP premises; and in the approved use of equipment in other organisations.

2.1 Users are defined as: all police officers, special constables, police staff, contractors, volunteers, and approved users (including individuals on secondment to, or from, other forces) with Force issued identification and passwords.

### **3.0 General Principles**

#### **3.1 Access to electronic communication systems**

Users are required to act within existing Force policies, national guidelines and legislation, and Force Electronic Communication Standards for each method of electronic communication.

##### **3.1.1 Security Risk Management**

Users should be aware that the Force has controls in place to monitor e-mail and internet traffic. These controls are required to ensure there is no security risk to the Force through malicious software, computer viruses, unauthorised access by hackers or unlawful disclosure.

##### **3.1.2 E-mail – internal and external**

Access to the Force e-mail system is available to users via Force approved terminals and remote access devices. E-mail is only for use by authorised users in the course of their duties. Occasional and reasonable personal use is acceptable. It is the responsibility of the person's line manager to determine what is reasonable or acceptable, in conjunction with the guidance provided in the attached e-mail standards.

3.1.3 The Force e-mail system works in conjunction with the internet so users must also comply with both the e-mail and internet standards.

3.1.4 All e-mails, sent or received, are records that belong to TVP. E-mails containing TVP documents (e-attachments) are also considered records (separate from the original document) as it is considered that the e-mail adds context to the attachment. E-mail records are encompassed by Data Protection and Freedom of Information legislation.

3.1.5 Inappropriate use of e-mail or transmission of inappropriate material via e-mail, that is pornographic, racist, threatening, harassing, bullying, sexist, insulting, offensive or discriminatory against an individual or group will compromise the Force and, may result in disciplinary action and may constitute a criminal offence.

### **3.2 Intranet**

Intranet access is available to all users via TVP desktop or remote access browsers, as approved by the ICT Department

3.2.1 The content of the intranet is for business use. Only authorised users are allowed to publish information, or create sites, on the intranet.

3.2.2 Users are permitted occasional and reasonable use of the intranet discussion forum. Users must comply with the rules of the discussion forum, as published on the forum. It is the responsibility of the user's line manager to determine what is reasonable, or acceptable use of the forum.

3.2.3 The forum administrators may remove items if they are considered to be inappropriate in the circumstances, or breach the discussion forum rules. Users who are considered to constantly mis-use or over-use the forum may have their access to the Forum removed. In exceptional circumstances disciplinary action may be considered.

### **3.3 Internet**

Internet access is allowed via ICT approved TVP desktop or remote access browsers; non-TVP approved internet service provider (ISP), on a stand-alone desktop or portable PC; on the understanding that these ISPs are not supported by the ICT Department.

3.3.1 Approved firewalls are required in all circumstances. The level of firewall required will be balanced against the Government Protective Marking Scheme (GPMS) level of data held on the device.

3.3.2 The Force uses software to protect the network from malicious software like viruses or spyware. Access to internet sites deemed 'unsafe' by the software will be prevented automatically. The software also prevents access to inappropriate sites with adult and sexually explicit material, racist or violent material, and other categories of sites; as determined by the policy owner.

Users should be aware that attempts to access 'blocked' sites are logged and subject to routine audit. Users may be asked to account for their actions.

3.3.3 Access to the internet is allowed on the condition that it is used as an appropriate business tool. This includes research for information relevant to the user's role and for the purpose of updating and publishing information on Force approved social networking sites. See appendix D for the social networking standard.

3.3.4 Personal use is permitted during a user's own time (during meal breaks/ before or after the working day) providing that, in the line manager's view, such usage does not affect the individual's performance in his/her day to day role; and on the understanding that the user conforms with the Force Electronic Communications Policy and Standards at all times.

### **3.4 Users' responsibilities**

All users should ensure they are familiar with the electronic communications policy and standards, and adhere to them at all times. Users should have access to the Microsoft Outlook manual on the use of e-mail.

<http://onlineview/training/workbooks/xpmanual.pdf>

### **3.5 Line managers' responsibilities**

Line managers must ensure their staff are aware of, and know they must comply with, the electronic communications policy and standards at all times, and have access to a copy of the Microsoft Outlook manual on the use of e-mail. <http://onlineview/training/workbooks/xpmanual.pdf>

3.5.1 Line managers should take appropriate action in the event of suspected misuse of the internet, intranet and e-mail facilities by a member of their staff, or when the level of personal use of the systems is considered to be unacceptable.

## **4.0 Guidance, Procedures & Tactics**

[Appendix A – E-mail Standards](#)

[Appendix B – Internet Standards](#)

[Appendix C – Intranet Standards](#)

[Appendix D – Social networking Standards](#)

## **5.0 Challenges & Representations**

Any challenges to this policy or recommendations for amendment should be addressed to:

Head of Corporate Communications, TVP Headquarters South, Kidlington,  
OX5 2NX

## **6.0 Communication Strategy**

This policy will be published on the Policy Management Unit intranet site and Force internet site. An entry will also be made in Managers' Briefing and Weekly Orders to advise all staff of the new policy and direct them to the policy on the Intranet site.

## **7.0 Compliance and Certification**

### **7.1 Human Rights Certification**

#### **a) Legal Basis**

- Data Protection Act 1998 including rights of subject access
- Computer Misuse Act
- ACPO Community Security Policy
- Force Information Security Policy
- Government Protective Marking Scheme
- Links to Police National Legal Database Other
- Defamation Act 1996
- Obscene Publications Act 1959
- Copyrights, Designs and Patents Act 1988
- Sexual Offences Act 1976
- Human Rights Act 1998
- Public Order Act 1986
- Crime and Disorder Act 1998
- Regulation of Investigatory Powers Act 2000
- Common Law of Libel and Defamation

#### **Human Rights Articles Engaged**

- Article 8 – Respect for private and family life
- Article 10 – Freedom of Expression
- Article 14 – Prohibition of Discrimination

#### **Prohibition of Discrimination**

Application of this policy could discriminate against individuals either directly or indirectly.

Article 14 states 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, nation or social origin, association with a national minority, property, birth or other status.

Unless there is an infringement of another article, Article 14 will not apply as it is not freestanding. However actions and decisions taken as a consequence of this policy could be judged to be discriminatory in employment law if they are not applied fairly and impartially, having due regard for natural justice and human rights.

### **7.2 Diversity Impact Assessment**

This policy has been assessed for having a low impact on the six strands of Diversity.

### **7.3 Diversity (Human Resources)**

In the application of this policy, the Force will not discriminate against any persons regardless of their gender, sexual orientation, race or ethnic origin, religion, age or disability.

### **7.4 Management of Police Information (MoPI)**

This policy and standards have been written with MoPI guidelines in view. A further review of the document will take place in Sept 2009 in conjunction with the Information Manager.

For further guidance on MoPI requirements please use the following link:

- [MoPI](#) - Why we have to comply with MOPI Codes of Practice and Guidance

**Alternatively please contact Information Management Department for advice and guidance.**

### **7.5 Community Engagement Strategy and Standards**

This policy does not have the potential to engage any of the Force Community Engagement Standards.

Please use the links for more information:

- [Community Engagement Strategy](#)
- [Standards](#)

### **7.6 Data Protection**

This policy reflects the legal obligations and responsibilities outlined in legislation governing electronic communication issues, and has been formulated after detailed consultation with the Force Information Security Officer, the Force Internal Communications Manager and the Data Protection Officer.

### **7.7 Freedom of Information Act**

This policy can be made available to the general public and will be published on the Policy and Procedures Freedom of Information internet site.

### **7.8 Protective Markings**

This policy has been assessed for its correct level of protective marking and is classified as NOT PROTECTIVELY MARKED

### **7.9 Health & Safety at Work**

This policy is to be read in conjunction with the Force Health and Safety Management Policy and Health & Safety Manual, which set out the requirement for documented risk assessment by a competent person, when exposure to a particular hazard arising from workplace or pre-planned policing work activity can be said to be reasonably foreseeable.

The Health, Safety and Welfare issues connected with this policy include;

- The need for supervisors to closely monitor their officers and staff, and ensure they are properly supported should they view any material that may cause offence or distress.

## **8.0 Monitoring and Review**

### **8.1 Links to Best Value/PPAF/Priorities/Performance Indicators**

### **8.2 Review Process**

A full review will be carried out by the policy author and will examine:

- Changes in legislation
- Court rulings – Domestic, European and Human Rights
- Examples of good practice from other Forces or other organisations
- Changes in Home Office Circulars
- Developments with ACPO Policy Unit
- Representations made by individuals and relevant organisations
- Relevant Equality data

### **FOR POLICY MANAGEMENT UNIT USE ONLY**

#### **Policy Authorisation**

**Policy signed off by:**

\_\_\_\_\_

**A/Director of Information & Strategy**

\_\_\_\_\_

**Date**

## **Thames Valley Police E- Mail Standard**

### **Introduction**

This E-mail Standard forms part of the Electronic Communication Policy and must be read and followed by you as a user of the Thames Valley Police e-mail system. Compliance with this standard is mandatory. The standard provides users with guidance on the use of e-mail and supervision of users, if applicable to their role.

### **Users and approved equipment**

Users include: police officers, special constables, police staff, contractors, volunteers and approved users who have been issued with a Force identification and password, and allocated a personal e-mail account. Personal e-mail accounts are allocated to new users by the ICT service desk.

The standard applies equally to the use of Force approved terminals and equipment inside and outside TVP premises; and in the approved use of equipment in other organisations. Users must ensure that, when using equipment provided by other organisations, they comply with the policies and procedures in place in that organisation.

E-mail usage has the potential to occupy significant amounts of users' time and users should focus on how to reduce the number of messages they send.

## **A – Z of standards**

### **All-user messages**

Messages to 'all Force e-mail users', 'all police officers' or 'all police staff' must be authorised by Corporate Communications. Authorisation is given if the message is judged to be relevant to all recipients in the group, or the message is urgent and requires immediate circulation.

Requests for messages should be forwarded to the 'All-user requests' mailbox; when authorised, the message will be circulated by Corporate Communications. A small group of staff also has permission to send Force-wide 'all user' messages, these include ICT Service Desk, HQ Operations and the Welfare Department.

Local all-user messages BCUs and departments have standard procedures for sending local all user messages. In most cases permissions have been restricted to senior managers and local communication teams.

### **Attachments**

Messages containing attachments should be kept to a minimum and must never be sent to large numbers of users. Where possible, a document can be published in an open file like an intranet page, and a link included in the e-mail message. E-mail **Internal Comms** for advice on saving documents as intranet pages. Only documents and data files may be attached to e-mail messages.

### **Authorisation**

E-mail distribution lists should be used responsibly. Only business messages should be sent to large numbers of staff. Senders should first check with their line managers to ensure they have authorisation to send messages to large numbers of users.

### **Business use, chain letters, political activities, buying and selling etc**

Users are prohibited from using the TVP e-mail system for private business purposes; buying or selling on internet auction sites; conducting political activities and fund raising. Chain letters should not be forwarded or initiated by users, to any e-mail address.

### **Copyright**

Users are prohibited from distributing or receiving unauthorised copyright materials. If users are unsure whether they are lawfully able to use a piece of software they can contact the ICT Service Desk for advice.

### **Disclaimers**

All e-mail messages should include a disclaimer. Users need to set up their own internal disclaimer; the external disclaimer is automatically included by ICT.

#### Internal disclaimer

This communication contains information that is confidential and may also be privileged. It is for the exclusive use of the intended recipient(s). If you are not the intended recipient(s) please note that any form of distribution, copying or use of this communication, or the information in it, is strictly prohibited and may be unlawful. If you have received this communication in error please return it to the sender. The content of this message may contain the personal views of the author and are not necessarily those of Thames Valley Police.

If a user feels there is any possible ambiguity as to whether a message they are sending is on their own behalf, or on behalf of the Force, they should include a statement to clarify which is the case.

### **Distribution lists for internal and external groups**

Check the names on any group distribution list before pressing send. The list may contain external recipients who are not cleared to receive the information. It is also good practice to double check the name of the list to make sure an external list hasn't been picked instead of an internal group with a similar name.

Distribution lists should be regularly reviewed and updated.

### **Forwarding e-mail messages – when out of office**

Setting up messages to be forwarded automatically to an address outside TVP (such as a home e-mail address) is prohibited. This is a fundamental breach of security. This is to ensure that sensitive information is not sent to a third party or passed via an unsecured network.

### **Full mailboxes**

When mailboxes are full undelivered messages are collected in the Postmaster's mailbox. If they are not claimed within seven days they are deleted. Check with ICT Service Desk if a particular message has not been received while an inbox was full.

### **Jokes, games and photos**

Electronic copies of non-work related images or photographs, jokes, or interactive computer games or programmes must not be received or sent; either internally or externally; or saved on Force drives.

### **Junk mail**

The Force spam filter prevents junk mail reaching inboxes and will send a message to the user to show what has been received. The user can then decide if the message can be deleted or not.

Junk mail messages should be deleted if it is not clear what the message contains. The offending e-mail addresses can also be added to the 'junk senders list' – any messages from those addresses will then delete automatically from the inbox.

Users should not attempt to 'unsubscribe' from receiving 'junk' messages. The act of unsubscribing makes the sender aware that the target mailbox is active and will result in more junk mail being received. For further advice contact the Force Information Security Officer.

### **Offensive or inappropriate messages**

If an e-mail is received from any source, which breaches this policy or is otherwise offensive or concerning, it should not be deleted or forwarded. Users should immediately contact their line manager and the Information Security Officer on 700 6594 and, **only if instructed to do so**, e-mail a copy of the message received to Information Security who will then commence an investigation.

### **Out of office messages**

All users must set up their own out of office message. It should provide information for the recipient to find an alternative contact to deal with their request, and to inform them when the person will be back at work.

Neighbourhood officers and Neighbourhood teams must also include details of the Force non-emergency number in their out of office messages. Other operational officers and staff should include the non-emergency number if the PEC call takers are able to deal with queries relating to their roles.

### **Passwords**

Users require their own personal identity and password which should never be divulged to anyone else. Users are personally liable for all messages sent from their ID and password and are subject to disciplinary procedures in the event of misuse. Users should not, under any circumstances, allow another person to use their workstation while they are logged on.

Any **unauthorised** attempt to read another user's e-mail is a security violation and will be subject to disciplinary action.

Password protected screensavers are incorporated into all LAN terminals. Users must 'lock' their workstations before leaving them unattended. This can be done by pressing Alt+Ctrl+Del, then pressing the return key.

### **Personal data**

Users are prohibited from disclosing other employees' personal data without the individual's consent. This includes home addresses, home telephone numbers and personal e-mail addresses.

### **Personal use of e-mail**

The Force allows a limited and reasonable amount of personal use of internal and external e-mail. Personal use means brief messages to make and confirm appointments, or to communicate brief or urgent messages. Attachments should not be included in personal messages.

This should be conducted outside of core office/shift hours (i.e. before and after work and during meal breaks). Personal use of the e-mail facilities must not affect the individual's responsibility to complete his or her work.

### **Quarantined messages**

Messages are quarantined when the system picks up a possible virus or threat to the network. Quarantined messages may be viewed first by ICT staff to check the message contents.

Attachments should not be opened unless they are from a trusted source. Viruses stored in e-mail attachments cause over 90% of computer virus infections. Users are prohibited from knowingly take any action which would expose TVP to malicious software or viruses

### **Rules, policies and legislation**

Users are required to act within existing legislation, National Guidance and Force policies e.g. Diversity in Employment policy, Data Protection Act 1998, Computer Misuse Act 1990 and Copyrights, Designs and Patents Act 1988 etc in relation to the content and use of the e-mail system.

The Chief Constable as well as the e-mail author can be subject to litigation (whether the communication is internal or external) if the recipient of a message or an attachment, or those who may view it; perceive it to be bullying, harassing, malicious, libellous, salacious, pornographic, sexist, racist etc; or is likely to cause offence or distress to an individual or group.

All e-mail is stored for a certain amount of time and can, in principle be read if required for investigative and disciplinary purposes. It is not TVP policy to routinely view e-mail traffic.

### **Security of messages and Force systems**

E-mail can be subjected to hacking or interception and is not private or secure; it is the most exposed form of communication.

Information classified as CONFIDENTIAL or higher must not be sent via e-mail. Queries on the transmission of secure e-mail should be directed to the Force Information Security Officer.

E-mail accounts take the form:

forename.surname@thamesvalley.pnn.police.uk, this may vary slightly for users with the same name.

#### E-mailing other forces and criminal justice agencies

The PNN address is a secure method for sending e-mails between police forces and other criminal justice agencies. Information up to, and including, RESTRICTED may be sent securely between two .pnn addresses.

#### E-mailing statutory partner agencies

When communicating with statutory partner agencies (CDRP) staff should always communicate via a secure e-mail network. The intended recipient should be asked to provide a secure e-mail address, these will include addresses containing NHS.net, NHS(n3), JARD, GSI, GCSX, GSX, CJSM and GSE descriptors.

If your message is to an e-mail address not included in the above list, you should inform the intended recipient that you are unable to include GPMS classified material or sensitive personal information in your e-mail. In rare, operationally urgent circumstances, the information can be sent after a dynamic risk assessment has been carried out.

A written record of the dynamic risk assessment must be made in each case, and stored as a record in the event of the Force having to justify what might be seen as a breach of the law and assorted codes of connection.

### **Signatures**

Signatures should be clear and free from graphics or other downloaded images and slogans. The message should be written in black, Arial font size 12, on a white background, not in italics. This will allow everyone to read the message easily and is especially important for people with disabilities who may not be able to see text written in certain colours or on coloured backgrounds. Wallpaper designs should not be used for the same reason.

#### Signatures should contain:

Name, rank and/or role, contact number/s and address

Neighbourhood officers and Neighbourhood teams must also include details of the Force non-emergency number in their signatures.

Other operational officers and staff should include the non-emergency number if the PEC call takers are able to deal with queries relating to their roles.

### **Subject access**

E-mail content is subject to the Data Protection Act 1998 and subject access provisions. This means that messages relating to an individual should be

06/04/10

relevant, accurate and appropriate. The individual, who is the subject of the message, has the right to see the information.

### **Training**

Distance learning workbooks are available from the IT Training Unit intranet site from this link <http://onlineview/training/workbooks/xpmanual.pdf>

### **Warning Messages**

If a message is received purporting to contain a warning about computer viruses, it should not be opened. The ICT Service Desk should be informed, and appropriate guidance will be given. They will inform Force Security as appropriate.

**Monitoring - This standard will be monitored along with the related policy at the time specified in the policy.**

## **THAMES VALLEY POLICE - Internet Standard**

### **Introduction**

This Internet Standard forms part of the Force Electronic Communication Policy and must be read and followed by all users. Compliance is mandatory. The standard provides staff and managers with clear guidance on the use, and supervision of users, of the internet facilities which includes the use of Force approved social networking sites. See appendix D for the social networking standard.

### **Users**

Users include all police officers, special constables, support staff, contractors, and volunteers and other approved users who have been issued with a Force identification and password.

### **General Principles**

#### **Internet use**

- Users must comply with the electronic communications policy and standards, and other related Force policies, at all times regardless of which device or equipment they are using to access the internet. This applies equally to 'stand alone' machines
- Users must only access the internet from their own LAN accounts.
- Each user is responsible for the internet activity that takes place while they are logged on.
- Users must not leave their computers unattended when they are 'logged on' and must use the 'alt+Ctrl+Del' function to ensure their workstations are secure when away from their desks.

### **Procedures**

#### **Improper or Inappropriate use**

The Force uses specialist software to track usage of the system, to block access to inappropriate sites and sites which represent a technical danger to the network. Users leave 'electronic footprints' as they travel round the internet, these can be tracked and used as evidence in any investigations into inappropriate use.

These footprints can also be used by the owner of an external website to identify that a member of TVP has accessed their site. If the internet is being used for investigation purposes users must be sure that any electronic footprint they leave will not compromise their investigation. Contact the Force Information Security Officer if in doubt.

#### **Internet facilities must not be used to:**

- Compromise the name and/or the reputation, or make unauthorised financial commitments of TVP
- Design or build a site in the name of TVP or represent personal views as those of TVP
- Intentionally retrieve or disseminate unsuitable or sensitive/private material

- Distribute or receive unauthorised copyright materials; download, print or re-use copyrighted materials
- Conduct a personal business enterprise; including buying or selling on auction sites.
- Conduct political activity.
- Use the Force website to fund raise unless authorised to do so.
- Make harassing or offensive statements, including any debasement of race, gender, national origin, sexuality, age, disability, religious or political beliefs.
- Access social networking sites unless this is part of an individual's role.
- Knowingly take any action which would expose TVP to malicious software or viruses
- Any action which is unlawful like downloading child pornography
- Access or attempt to access streaming media such as music sites, TV, radio, video etc.
- Access to some sites can be authorised for operational purposes, users should contact the Force Information Security Officer for advice.

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

### **Consequences of inappropriate or improper usage**

The Force Security Department conducts regular audits of Internet usage. Line managers will be contacted in the event of apparent excessive use or habitual attempts to access 'barred' sites.

If line managers suspect excessive or inappropriate use they will be provided with a copy of internet usage reports for their staff, on request, from the Force Information Security Officer. Users must be aware that reports will include references to all sites they have visited and that such a disclosure could constitute 'sensitive personal data'.

Internet facilities can be removed on the authority of a line manager and Human Resources Department. This removal of access can be permanent or temporary and will usually be requested in conjunction with other disciplinary or performance related matters.

Disciplinary procedures up to and including dismissal, will be considered in all cases where inappropriate use is detected. In cases where criminal or serious disciplinary matters are apparent the matter will be referred to the Professional Standards Department.

### **Web access**

Any message that passes through the internet gateway uses bandwidth on the Force network. High volumes of traffic could potentially affect the overall service. One user could not provoke such a load on the system with two possible exceptions:

- Downloading large files from the internet. If files are needed for work purposes they should be downloaded onto a standalone machine or at a time when there is less demand on the LAN. Consult the ICT Service Desk.
- Signing up to any site like a talk group that generates large numbers of responses and/or attachments. If such subscriptions could be useful for work purposes users should first seek approval from their line manager who will need to inform the ICT Service Desk and Force Security. The volume of traffic can then be monitored accordingly.

Do not attempt to download any software. If software is needed for a particular role an individual's line manager must first approve the request. ICT will check the software to ensure it is compatible with the network and that licensing and security issues are satisfied. Budget approval will be required to cover the costs of support, maintenance and purchase of software and/or copyright licences.

Permission must be sought before using or circulating any copyrighted material. This material can be identified by a copyright logo or a statement from the owner. First contact ICT Service Desk for advice.

### **Security**

Force policy is to block access to particular sites and categories of sites to protect the reputation of TVP and the security of the network. A list of prohibited sites is maintained by Force Security. Should there be a site that is blocked unnecessarily it should be reported to the ICT Service Desk.

Anyone who needs to access 'blocked' sites as part of their role must discuss their requirements first with their line manager and contact the ICT Service Desk for further advice

### **Monitoring**

**This standard will be monitored along with the related policy at the time specified in the policy.**

## **Appendix C**

### **THAMES VALLEY POLICE - Intranet Standard**

#### **Introduction**

This Intranet Standard forms part of the Electronic Communications Policy and must be read and followed by all users. Compliance is mandatory. The standard provides staff and managers with clear guidance on the use, and supervision of the use, of the intranet facilities.

**Users** include all staff: police officers, special constables, support staff, contractors, volunteers and approved users who have been issued with a Force identification and password. The intranet is available via Force approved terminals and approved remote access devices.

#### **General Principles**

- Users must comply with the electronic communications policy and standards, and other related Force policies, at all times regardless of the device or equipment they are using.
- Each user is responsible for the intranet activity that takes place while they are logged on. Users should only access the intranet from their own LAN logon.
- Users must not leave their computers unattended and must use the 'Alt+Ctrl+Del' function to secure their workstation when away from their desks.
- The Intranet Forum is available for ad-hoc sale and purchase of approved items.

#### **Users must not:**

- Download or publish unauthorised copyright materials
- Conduct political activity or use the intranet for private business purposes.
- Make harassing or offensive statements, including any debasement of race, gender, national origin, sexuality, age, disability, religious or political beliefs.
- Copy and circulate information from intranet pages/attachments unless to authorised, approved and trusted sources.

#### **Publishers**

Only fully trained and authorised users can publish information on the intranet using Force approved computers. Articles for publication should be authorised first then forwarded to a local publisher or to the Internal Communications Team in Corporate Communications.

Users who contribute to the intranet discussion forum are required to comply with the rules of the forum and act within existing Force policies and current legislation in relation to the content and use of the system. The forum rules are available on the forum.

#### **Monitoring**

**This standard will be monitored along with the related policy at the time specified in the policy.**

## **Appendix D**

### **THAMES VALLEY POLICE - Social Networking Standard**

#### **Introduction**

The Social Networking Standard forms part of the Electronic Communications Policy and must be read and followed by all users. The intention of the standard is to provide staff and managers with clear guidance on how to set up and manage an official Thames Valley Police social networking site and supervise users.

#### **Users**

Users include all police officers, special constables, support staff, contractors and volunteers and other approved users who have been issued with a Force identification and password. Users must comply with the e-communications policy and all other relevant Force policies at all times.

#### **Rules for all TVP Social Networking sites**

##### **Getting started**

New official TVP social networking pages must be approved first by the Head of Corporate Communications before any pages are created to ensure the site complies with these standards. Site owners must demonstrate that the pages meet a clear business need.

The team/department concerned will be responsible for the management of its content and must update it regularly. A content owner and deputy must be nominated when the site is set up and plans put in place to maintain/monitor the site when they are unavailable.

##### **All TVP pages should include the following prominently:**

- A link to the TVP website
- Information on how to report a crime (and an explanation that should people want to report a crime or name suspects, they should do it by phoning the appropriate number and not by posting it on social networking sites, and not to name anyone they suspect of a crime)
- A request for people not to post offensive or abusive content

##### **Dealing with negative comments**

- Respond to them reasonably and promptly and forward to the correct Force contact if appropriate
- Remove comments if they are clearly malicious, offensive, abusive or legally suspect.

##### **Users must ensure that:**

- All content – text, photos, videos etc - are in line with the Force's corporate position.

- Nothing is posted that could bring the Force into disrepute or conflict with our corporate message or style; compromise an operation, or jeopardise a court case.
- All current TVP videos for external consumption will be posted on YouTube
- Any photographs or video posted on social networking or image sharing sites serve a policing purpose and comply with legal or data protection requirements.
- All e-mail messages from social networking sites are being acted on promptly, and a response posted as quickly as possible after consultation with an appropriate member of staff.
- Any appeals for wanted or missing people must link to the Force website so that images can be removed promptly once people are found.

### **Neighbourhood team pages**

The page name should be clearly identified as a Thames Valley Police site and the name of the neighbourhood should also be prominent.

In a prominent place on the page, there should be:

- A link to the relevant NH page on the TVP website
- There should be guidance on how to report crime (999 in emergencies, otherwise 0845 8 505 505)
- There should be advice on what can and can't be posted on the page (no reporting of crime, no intelligence, no naming of individuals, nothing abusive or derogatory etc)
- Links to local partners' sites
- A member of the team should post something of interest on the page at least once a day, check posts from 'friends', check for inappropriate comments and ensure comments and profile status are still relevant.
- Out-of-date content must be removed as soon as possible.

### **Reactive use of non-TVP social media sites**

The public social networking sites should be monitored regularly for non-TVP social networking sites containing tributes to murder victims or that urging vigilante action against certain offenders.

We should post on pages of non-TVP social networking sites only if at least one of the following criteria is satisfied:

- There is a direct request from the SIO to use this media.
- There is an opportunity to address trust and confidence issues.
- There is an opportunity to seek information, intelligence and evidence.
- We only use information that is already in the public domain.
- We do not enter into a dialogue on the site.

We should not interact with the public on pages that are purely negative about the police (such as "we hate TVP")

### **Reviewing the site**

Corporate Communications will have access to all corporate sites. Regular reviews will be carried out to assess the appropriateness of the various TVP social networking content. Content will be removed, as necessary and the owner informed accordingly. Accounts should not be deactivated without informing Corporate Communications first.

### **Monitoring the sites**

Thames Valley Police's use of social networking will be reviewed and evaluated at regular intervals to ensure that we are:

- Garnering enough benefit from using social media
- Using our resources effectively
- Not compromising the reputation of the Force.