Policy Title: Electronic Communications Policy

Date Reviewed: January 2020

Thames Valley Police ensures that all policies have been assessed and comply with MoPI Guidance, and the Data Protection Act 2018. In addition, this Policy has been reviewed by the Force Head of Health, Safety and Environment and has undergone an Equality Impact Assessment.

1.0 About this Policy

1.1 Rationale

This policy covers the use of all Force electronic communication systems both internal and external that are provided for business purposes. These include the intranet, internet, social media, e-mail and facsimile, and any process that uses these systems as an operating platform such as blogs, Facebook, YouTube, Twitter or Yammer.

1.2 Legislation/National Standards

- Data Protection Act 2018 including rights of subject access Computer Misuse Act
- Freedom of Information Act 2000
- ACPO Community Security Policy Force Information Security Policy
- Government Security Classification Policy
- ACPO Publication Scheme
- 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

1.3 Intention

The intention of this policy is to give staff and managers clear guidance on the use, and supervision of users, of these systems.

1.4 General Principles

The policy applies equally to users of Force approved terminals and mobile devices as well as other electronic devices inside and outside TVP premises; and in the approved use of equipment in other organisations. 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. 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 Statement of Policy

Access to Electronic Communication Systems

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

Security Risk Management

2.2 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, unauthorised users or unlawful disclosure.

E-mail – Internal and External

2.3 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.

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

2.5 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.

2.6 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, may result in disciplinary action and may constitute a criminal offence.

2.7 Access to a user's email account by a line supervisor or manager will be permitted in the absence and without the knowledge of the account holder, where it is necessary for the effective operation of the organisation's business. Applications for access will be made to the ICT Service Desk then to the requestor's line manager

for approval. For covert staff this may be referred to the Head of Information Management for authority to proceed and the ICT Service Desk will service the request once authorised. The member of staff will be informed at the earliest opportunity that the account has been accessed and why.

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

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

Internet
2.10 Internet access is allowed via Force approved TVP desktops, laptops 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 Force.

2.11 Approved firewalls are required in all circumstances. The level of firewall required will be balanced against the Government Security Classification (GSC) level of data held on the device.

2.12 The Force uses software to protect the network from malicious code 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.

2.13 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 Social Networking Standard.

2.14 Personal use is permitted during a user's own time (during meal breaks / before or after the working day, etc.) 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. Further information can be found in the Internet Access Policy

Fax Usage
2.15 When there is a requirement to send information to other criminal justice agencies or third-party organisations it is preferential that information be scanned and emailed using a secure e-mail address (PNN, GSI. GSX, CJSM). If a Fax is to be used only papers GSC classified no higher than Official can be sent without additional measures. Additional measures as detailed below (2.17) may need to be adopted depending on the sensitivity of the contents.

2.16 Personal information (that which identifies a living human being) and information classified with an Official-Sensitive handling caveat, that is information which through accidental or deliberate compromise would pose a risk to an individual's personal safety or liberty, hinder the detection of or impede the investigation of a low level crime, undermine confidence in public services or fail to maintain the confidence of those providing material - e.g. PNC print out, witness statement, should only be sent in cases of operational urgency and if due caution is exercised.

Due caution includes:
2.17 Verification that the fax number of the recipient is active and belongs to the intended recipient (telephone confirmation). Verification that the correct number has been dialled prior to sending any material (two people to check - one preferably in a supervisory capacity)

- That the standard force Fax front sheet is completed.
- That a test page is sent prior to the information being transmitted to ensure the recipient's machine is available to receive the information.
- Telephone confirmation that the test page had been received.
- Telephone confirmation that all pages of the transmitted 'Official / Official - Sensitive' material has been received by the intended recipient.
- A record is kept of time date and detail of the 'Official - Sensitive' information is transmitted.

Passwords
2.18 Users of ICT systems will be issued with unique usernames to access the systems. These will have an initial password which must be changed prior to using the system. Passwords are unique to a user and must not be shared with other members of staff, if you believe your password to have been compromised you should change it immediately. Details relating to password requirements can be found in Appendix E.

USB devices
2.19 Use of USB devices is restricted by default but certain business requirements, such as transfer of data, permit the use of approved encrypted devices. Requests for an encrypted memory device should be via the ICT Service Desk with a brief use case included. Further information can be found in the USB Standard (Appendix F).

IT Security
2.20 In order to minimise the risk of malware attack and data loss the safe and secure operation of IT is detailed in the ICT Security Induction.

Mobile Devices
2.21 Mobile devices have become an important tool in daily life but with the increase in mobility of data there are also new challenges to ensure the information being handled remains secure. Further information can be found in the Use of Mobile Devices policy.

Recording Devices
2.22 Unauthorised covert recording of colleagues or meetings is not permitted using

any devices. This will usually be a breach of the standards of professional behaviour and amount to misconduct.

Users' Responsibilities
2.23 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 any available Microsoft Outlook training on the use of e-mail.

Line Managers' Responsibilities
2.24 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 any available Microsoft Outlook training on the use of e-mail.

2.25 Line managers should take appropriate action in the event of suspected misuse of the internet, intranet, Social Media 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.

3.0 Human Rights Articles Engaged

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

4.0 Health and Safety at Work

4.1 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.

4.2 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.

5.0 Communications, Challenges and Representations

5.1 Communication

This policy shall be published on the TVP intranet site and the public website. 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.

5.2 Challenges and representation

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

Head of Corporate Communications,
Thames Valley Police Headquarters South,
Oxford Road
Kidlington
OX5 2NX

6.0 Review Date

January 2021

A full review shall be carried out at least every 3 years and shall 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
- ACPO policy development and Authorised Professional Practice
- Representations made by individuals and relevant organisations
- Relevant Equality data

7.0 Related Guidance

Appendix A – E-mail Standard
Appendix B – Internet Standard
Appendix C – Intranet Standard
Appendix D – Social Networking Standard
Appendix E – User Password Standard
Appendix F – USB Standard

8.0 Freedom of information

Suitable for publication.

9.0 Government Security Classification Policy

Official

10.0 Relevant Supporting information

Internet Access Policy
ICT Security Induction
Use of Mobile Devices policy