WEST MIDLANDS POLICE
Force Policy Document

POLICY TITLE:	**Acceptable Use Policy**
POLICY REFERENCE NO:	**Inf/27**

Executive Summary.

The primary aim of this policy is to set out the rules and conditions regulating the use of Internet, E-mail and Internet browsing access from computer terminals connected to the Force Wide Area Network (including Mobile & Remote Working devices). Also covered are conditions of use for the force telephone network and issued mobile telephones.

In keeping with the objectives to inspire public confidence in the Forces ability to protect the integrity and confidentiality of information assets and demonstrate commitment to maintaining professional standards, these rules and conditions are considered appropriate and necessary measures to:

• Minimise the risk of information assets being compromised

• Minimise the risk of damage or disruption to the Force Wide Area Network

• Ensure compliance with legislative, regulatory, contractual, organisational and ethical requirements

• Maintain professional standards with regard to the content of electronic mail transmitted across or from the Force Wide System

• Maintain professional standards with regard to Internet browsing

• Maintain security and professional standards with regards to the use of the force telephone system

This Policy is issued to complement other Force Information Security policy documents.

***Any enquiries in relation to this policy should be made directly with the policy contact / department shown below.*

Intended Policy Audience.

This policy applies to every police officer, member of police staff, police community support officer, special constable, volunteer, contractor, and approved persons working for or on behalf of West Midlands Police.

Current Version And Effective Date.	**Version 0.1**	**2 March 15**
Business Area Owner	**Information Management Services**	
Department Responsible	**Information Management**	
Policy Contact	**Kate Jeffries – Head of Information Management**	
Policy Author	**Tom King – Information Security Officer**	
Approved By	**DCC Thompson**	
Policy Initial Implementation Date	**20/04/2015**	
Review Date	**20/04/2017**	
Protective Marking	**Not Protectively Marked**	
Suitable For Publication – Freedom Of Information	**Yes**	

Supporting Documents

- HMG Security Policy Framework (SPF);
- CESG IA Standards (IAS) and Good Practice Guides (GPG's);
- BS ISO 27001:20013 – Information Technology
- Security Assessment for Protectively Marked Assets (SAPMA)
- WMP Local Threat Assessment
- *Code of Ethics (http://www.college.police.uk/docs/Code_of_Ethics.pdf)*

Evidence Based Research

Full supporting documentation and evidence of consultation in relation to this policy including that of any version changes for implementation and review, are held with the Force Policy Co-ordinator including that of the authorised original Command Team papers.

Please Note.
PRINTED VERSIONS SHOULD NOT BE RELIED UPON. THE MOST UPTO DATE VERSION OF ANY POLICY OR DIRECTIVE CAN BE FOUND ON THE EQUIP DATABASE ON THE INTRANET.

Force Diversity Vision Statement and Values

"Eliminate unlawful discrimination, harassment and victimisation. Advance equality of opportunity and foster good relations by embedding a culture of equality and respect that puts all of our communities, officers and staff at the heart of everything we do. Working together as one we will strive to make a difference to our service delivery by mainstreaming our organisational values"

"All members of the public and communities we serve, all police officers, special constables and police staff members shall receive equal and fair treatment regardless of, age, disability, sex, race, gender reassignment, religion/belief, sexual orientation, marriage/civil partnership and pregnancy/maternity. If you consider this policy could be improved for any of these groups please raise with the author of the policy without delay."

Code of Ethics

West Midlands Police is committed to ensuring that the Code of Ethics is not simply another piece of paper, poster or laminate, but is at the heart of every policy, procedure, decision and action in policing.

The Code of Ethics is about self-awareness, ensuring that everyone in policing feels able to always do the right thing and is confident to challenge colleagues irrespective of their rank, role or position

Every single person working in West Midlands Police is expected to adopt and adhere to the principles and standards set out in the Code.

The main purpose of the Code of Ethics is to be a guide to "good" policing, not something to punish "poor" policing.

The Code describes nine principles and ten standards of behaviour that sets and defines the exemplary standards expected of everyone who works in policing.

Please see http://www.college.police.uk/docs/Code_of_Ethics.pdf for further details.

The policy contained in this document seeks to build upon the overarching principles within the Code to further support people in the organization to do the right thing.

CONTENTS

1. INTRODUCTION.

1.1 The primary aim of this policy is to set out the rules and conditions regulating the use of Internet, E-mail and Internet browsing access from computer terminals connected to the Force Wide Area Network (including Mobile & Remote Working devices). Also covered are conditions of use for the force telephone network and issued mobile telephones.

2. ACCEPTABLE USE POLICY

2.1 Applicability

2.1.1 This policy applies to all Police Officers, Police Staff, Special Constables, Volunteers and all contracted third parties, whether they are working on Force premises, in their offices or from home. It is supplementary to the Force Information Security Policy and other security requirements.

2.1.2 **Compliance with this policy is mandatory**. Failure to comply may result in:

- Legal claims against West Midlands Police
- Legal claims against individual users
- Withdrawal of Internet facilities
- Disciplinary action
- Criminal proceedings

2.2 Legal Basis and Driving Force

2.2.1 External threats have the potential to disrupt the designed functionality of all or parts of the Force Wide System and present onward transmission risk to other users of the Criminal Justice Extranet. The following are the main references that mandate the provisions of this policy:

- HMG Security Policy Framework Tier 1-3
- Security Policy and Code of Connection for the CJX
- The ACPO/ACPOS Information Systems Community Security Policy
- The Data Protection Act 1998
- The Computer Misuse Act 1990
- The Official Secrets Act 1911 – 1989
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- The Regulation of Investigatory Powers Act 2000 (RIPA)

2.3 General Principles

2.3.1 Personnel are able to use the Internet, email and telephone systems for West Midlands Police business use and appropriate personal use as described throughout this document. The general principles are that users must:

- Use the facility in a responsible manner
- Comply with all existing Information Systems and Information Security policies
- Ensure they are aware of their personal responsibilities
- Not access unsuitable material
- Not use the systems during working time for non-work related issues

2.3.2 Permission to use the internet may be withdrawn if personal use adversely affects official use. This will be determined by Line Managers

2.4 The Internet

2.4.1 The Internet is a worldwide network providing a global infrastructure over which anyone can send data or make data available in electronic format. Whilst this presents considerable opportunities for the West Midlands Police to benefit from the full potential of electronic communications, the Internet is largely unregulated and the risk from malicious activity directed at the Force is significant. This risk can be reduced to acceptable levels through the application of technical measures and adherence to user rules and conventions, some of which are specific to this policy.

2.5 WMP Good Email Practice Guide

2.5.1 The following guidelines represent good practice when using e-mail:

- Obtain confirmation of receipt of important e-mails, particularly those containing personal data.
- Check e-mail accounts each working day.
- Reply promptly to e-mail messages requiring a response. Where prompt response is not practicable, an acknowledgement should be sent.
- When sending emails, authors should be mindful that the content of their email is consistent with the Standards of Professional Behaviour. Specifically they must demonstrate respect and courtesy towards the public and colleagues and they must treat all information with respect and disclose it only in the proper course of police duties,
- It is not acceptable to send emails to personal email accounts or home computers that relates to West Midlands Police or criminal investigations.
- Regularly weed e-mail folders to ensure messages and attachments are retained no longer than necessary.
- Ensure outgoing e-mail is accurately addressed.

- Report any suspicious or unsolicited mail (junk mail in electronic format – mainly offering goods or services) to the ICT Helpdesk without delay.

- When on annual leave or away from the office for a substantial period, use the "Out of Office Assistant" to notify the sender of the mail your whereabouts, your expected date of return and who they could contact in your absence. Alternatively you can automatically forward your mail to a colleague authorised to deal with it in your absence. Under **NO** circumstances should you auto forward e mail to your home email address

2.6 SMS Messaging System

2.6.1 The relevant parts of this policy that refer to E-mail use also apply to the use of the SMS messaging facility on the Force Wide System.

2.7 External Communications Standards

2.7.1 With regard to professional standards, Internet E-mail must be viewed in the same context as other means of external communications such as letter, fax and telephone. Users must appreciate that E-mail transactions have the same legal standing as a letter on headed paper. Content, quality and promptness of response equally apply.

2.8 Force Landlines and Mobile Telephone Systems

2.8.1 The following information relates to the fixed Public Switched Telephone Network (PSTN – Force landlines) and issued mobile telephones. It must be noted that the threats to mobile telephones apply to all devices, not only those issued by the West Midlands Police Police.

Landlines

2.8.2 All telephone users must be aware that any speech over the PSTN is at risk of interception by unauthorised persons or groups and guard their speech accordingly.

2.8.3 If there is an operational requirement for information at RESTRICTED to be discussed over the PSTN, both the sender and the receiver must accept the risk.

2.8.4 Information at CONFIDENTIAL level or higher should not be discussed over the PSTN and should only be transmitted over a secure telephone network.

2.8.5 When using the telephone system, users should apply the general principles of this document, along with the Acceptable and Unacceptable standards outlined in the paragraphs below.

2.8.6 When on annual leave or away from your desk for a substantial period of time make use of the voicemail facility to notify the caller of who's phone they have reached and invite them to leave an unclassified message or direct them to another person who is authorised to receive your calls.

Mobiles

2.8.7 Within the UK there is a threat of mobile phone exploitation, especially where sensitive issues are discussed. The threat overseas is much higher than within the UK.

2.8.8 Mobile phones are vulnerable to accidental activation while they are switched on and some modern generation phones can be active even though they appear to be switched off. There are even commercial eavesdropping products that can be dialled using a special access number.

2.8.9 Data stored on a mobile phone is vulnerable to compromise, especially on disposal, unless deliberate steps are taken to erase the information.

2.8.10 Most mobile phones come with a Bluetooth or Infrared (IR) link which may be open to compromise, making it possible to remotely access phone functions, alter them and download data.

2.8.11 Phones may also be fitted with a camera, raising the potential for the unauthorised capture of information. To mitigate the treats to mobile phones it is recommended that the business use of mobile telephones is regulated in line with this policy:

- Where practicable, mobile telephones used by staff employed within sensitive departments should be changed regularly (including the SIM), ensuring that no details of the new telephone are passed to the old one – e.g. using the old phone to inform contacts of the new number.
- Where possible, block procurement with sequential numbers should be avoided.
- Telephones should not be left unattended and insecure.
- Local asset control procedures should include methods of controlled disposal or sanitisation of reissued telephones.
- Telephones should not be used for sensitive conversations where there is a risk of being overheard.
- The use of Bluetooth or IR should be disabled or the risk of compromise accepted by the user.
- Where practicable, mobile telephones are forbidden from areas where highly sensitive information is discussed on a regular basis.
- There is an expectation for calls made for private use to be paid for by the individual making the calls. Please see the Business Expenses and Travel Policy owned by HR for more details.

2.9 Acceptable Use

2.9.1 Internet, E-mail and telephone services are primarily provided for official police purposes only. However, occasional and reasonable personal use of these services will be permitted during authorised break periods or out of hours provided that such use does not interfere with official business or the performance of official duties and responsibilities. **Such interference will be determined by Line Managers.**

2.9.2 Examples of acceptable use include, but are not limited to:

- Policing purposes.
- Browsing web sites for goods or services, for example, holidays or theatre tickets.
- Reasonable and limited use of bulletin boards, social networking groups (e.g. Facebook, Twitter etc), newsgroups or chat rooms. (See Section 2.11)

2.10 Unacceptable Use

2.10.1 Internet access and E-mail will not be used for:

- Personal business purposes or commercial financial gain. Downloading or copying material in breach of copyright licensing.
- The sending of whole force email unless approved by an authorised person
- Downloading software of any description.
- Seeking, retrieving, displaying or downloading data in any format which is indecent, offensive, subversive, illegal or otherwise inappropriate and inconsistent with Force Professional Standards.
- Creating or using e-mail accounts other than the one provided by the ICT Department or accessing Internet based accounts (e.g. Hotmail, AOL, Yahoo, etc).
- Registering Force email addresses with commercial websites for personal purposes.
- Accessing and using on-line computer games.
- Engaging in political activity (Police Federation and Unison representatives communicating with Staff on legitimate business are not included in this section).
- Authoring, transmitting or storing messages or attachments containing racist, sexist, defamatory, offensive, abusive, illegal or otherwise inappropriate words or material.
- Circulating chain mails.

- Engaging in or creating binding contracts unless authorised to do so in support of formally approved procurement procedures. All final versions of any contracts must be signed in hard copy format.
- Transmitting unencrypted information protectively marked RESTRICTED or above over the Internet.
- Excessive personal use of Internet browsing facilities (To be determined by Line Managers measured against any adverse impact on official use).
- Excessive personal use of email messaging facilities. (To be determined by Line Managers measured against any adverse impact on official use).

2.11 Advice and Guidance on use of Social Networking Sites

2.11.1 When using Social Networking Sites (either for personal or Force business use) the Standards of Professional Behaviour for Police Officers and Police Staff should be taken into consideration.

2.11.2 Advice and Guidance on the use of Social Networking Sites will be issued from time to time and can be found in the **Guidance for Police Personnel – Use of Online Social Networking Websites** document.

2.12 Electronic Transmission of Personal Data Abroad

2.12.1 With the global messaging opportunities presented by Internet based email users are specifically reminded that they must adhere to Principle 8 of the Data Protection Act 1998 which states “Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data‟. The Force Disclosure Manager should be contacted if further information is required.

2.13 Non Conformance and Exceptions

2.13.1 Non-conformance to this policy must be reported to the relevant team. Information Security, Risk and Privacy must approve, track and report all exceptions to this policy in accordance with a formal documented process. The process should include a method for escalating significant exceptions that may breach a documented level of business risk tolerance, to appropriate boards and committees in accordance with established governance procedures for review and mitigation or formal risk acceptance

3. MONITORING, INTERCEPTION AND AUDIT

3.1 West Midlands Police reserves the right to monitor all communications (including telecommunications) using Force communications systems and where appropriate inspect the content of E-mail transmissions and Internet browsing sessions. Such activity is considered necessary for the purposes of:

- Protecting the network from malicious software, denial of service attacks and other external threats.

- Investigating and detecting improper use - preventing and detecting crime.
- Monitoring compliance with legal and regulatory requirements - ensuring that Staff comply with rules governing the use of communications systems.
- Quality control and training.
- Monitoring load level activity to ensure adequate technical provision of the service.

3.2 **AS SERVICES ARE PRIMARILY FOR BUSINESS PURPOSES, USERS MUST UNDERSTAND THAT THERE IS NO EXPECTATION OF PRIVACY.**

3.3. RIPA establishes a basic principle that communications may not be intercepted without consent and ensures compliance with ECHR and fundamental freedoms. The Lawful Business Practice Regulations make an exception to RIPA and allow businesses (including public authorities) to intercept communications transmitted across their systems without consent for certain purposes.

3.4. The monitoring and recording of communications will be considered on a case by case basis and will be used for:

- An appropriate method of ascertaining standards.
- To prevent or detect crime.
- To investigate or detect unauthorised use.

3.5. The Force Professional Standards Department is authorised to carry out the appropriate auditing of system use.

3.6. On application, an authority to proactively monitor or record specific communications utilising Force communication systems must be given by the Deputy Chief Constable or the Chief Constable in their absence.

3.7. Commanders and Departmental Heads are responsible for ensuring that all personnel who may use Force information and communication systems within their area of responsibility are aware of this authority and notice.

3.8. In all cases, regulations require the Force to make all reasonable efforts to inform every person using or who may use the system that monitoring and audit may take place. Accordingly, all potential users of Force communication systems are informed that:

- You work within an organisation that deals with sensitive matters and information, much of which is protectively marked.
- You are required to maintain the highest professional and ethical standards.
- To ensure that these sensitivities and high standards are maintained, communications by all users using Force information and communications systems (including but not limited to telephone, radio and E-mail) may be monitored and recorded

- Conversations conducted by all staff, contract employees and others who may use Force information and communication systems may not be considered to be private.
- When appropriate, recorded communications will be used in administrative, misconduct and criminal proceedings.

4. BREACH OF POLICY ESCALATION PROCEDURES

4.1 Purpose of Procedures

4.1.1 The purpose of these procedures is to ensure proportional and uniform action is taken in response to all breaches of Force Information Security Policies and associated Security Operating Procedures. They apply to both routine random monitoring and user specific monitoring requests. **All breaches will be dealt with under the Force Discipline Policy.**

4.2 Roles and Responsibilities

4.2.1 The Professional Standards Department is responsible for conducting monitoring and audit of Force information systems.. The ICT Department will provide technical assistance as appropriate for monitoring activities requiring additional technical support.

4.2.2 Potential policy breaches discovered by ICT Department staff during normal system administration must be reported to the Protective Security Manager in the first instance.

4.2.3 Line managers are responsible for ensuring compliance with Force polices through routine supervision of staff use of Force information systems.

4.2.4 The Deputy Chief Constable has authorised the Professional Standards Department to undertake routine random monitoring of Force systems to ensure that appropriate and proportionate monitoring and audit procedures are in place.

4.2.5 Requests for specific additional monitoring of an individual member of staffs use of Force systems must be made through formal application (Form 840).

4.2.6 **Before the Professional Standards Department undertake specific proactive monitoring requests they must be authorised by the Head of the Anti-Corruption Unit within Professional Standards for requests concerning Police Officers or the Head of Human Resources for requests concerning Police Staff.**

4.2.7 The results of monitoring undertaken in respect of authorised specific requests will be supplied to the requesting individual in the first instance. It is incumbent on that individual to take advice from the Head of Professional Standards or Head of Human Resources before proceeding with any form of administrative or disciplinary action.

4.3. Records

4.3.1 In cases where criminal conduct is being investigated, Professional Standards will maintain monitoring records.

5. AUTOMATED RESTRICTIONS

5.1 To enable the Head of IST to provide an efficient service, automated restrictions are deployed on the network. These will include virus scanning and content checking of electronic data received from external sources and denying access to some Internet web sites. A small number of key post holders have unrestricted Internet access to fulfil intelligence gathering or other operational requirements.

6. UNDERPINNING POLICIES AND PROCEDURES

6.1 To support the overarching IA Risk Management policy the following policies will be maintained by the force:

1. Force Information Security Policy;
2. Information Services Risk Register;
3. West Midlands Police Risk Appetite Statement;
4. Force Information Risk Management Policy
5. Information Sharing Agreement Policy
6. Guidance for Police Personnel Use of Online Social Networking Websites

7. EQUALITY IMPACT ASSESSMENT (EQIA).

7.1 The policy has been reviewed and drafted against all protected characteristics in accordance with the Public Sector Equality Duty embodied in the Equality Act 2010. The policy has therefore been Equality Impact Assessed to show how West Midlands Police has evidenced 'due regard' to the need to:

- Eliminate discrimination, harassment, and victimisation.
- Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it.
- Foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

Supporting documentation in the form of an EQIA has been completed and is available for viewing in conjunction with this policy.

8. HUMAN RIGHTS.

8.1 This policy has been implemented and reviewed in accordance with the European Convention and principles provided by the Human Rights Act 1998. The application of this policy has no differential impact on any of the articles within the Act. However, failure as to its implementation would impact on the core duties and values of West Midlands Police (and its partners), to uphold the law and serve/protect all members of its community (and beyond) from harm.

9. FREEDOM OF INFORMATION (FOI).

9.1 Public disclosure of this policy document is determined by the Force Policy Co-ordinator on agreement with its owner. Version 0.1 of this policy has been GPMS marked as Not Protectively Marked.

9.2 Public disclosure does not automatically apply to supporting force policies, directives and associated guidance documents, and in all cases the necessary advice should be sought prior to disclosure to any one of these associated documents.

Which exemptions apply and to which section of the document?	Whole document	Section number
N/A		

10. TRAINING.

10.1 There is no specific training for West Midlands Police personnel; however those individuals with a specific involvement in systems management will have the relevant training courses detailed within their job specifications.

11. PROMOTION / DISTRIBUTION & MARKETING.

11.1 The following methods will be adopted to ensure full knowledge of the Policy:

- Newsbeat
- Intranet
- Posters
- Policy Portal

11.2 No uncontrolled printed versions of this document are to be made without the authorisation of the document owner.

12. REVIEW.

12.1 The policy business owner – Head of Information Management – maintains outright ownership of the policy and any other associated documents and in-turn delegate responsibility to the department/unit responsible for its continued monitoring.

12.2 The policy should be considered a 'living document' and subject to regular review to reflect upon any Force, Home Office/ACPO, legislative changes, good practice (learning the lessons) both locally and nationally, etc.

12.3 A formal review of the policy document, including that of any other potential impacts i.e. EQIA, will be conducted annually as indicated on the first page.

12.4 Any amendments to the policy will be conducted and evidenced through the Force Policy Co-ordinator and set out within the version control template.

12.5 Feedback is always welcomed by the author/owner and/or Force Policy Co-ordinator as to the content and layout of the policy document and any potential improvements.

CHIEF CONSTABLE

13. VERSION HISTORY.

Version	Date	Reason for Change	Amended/Agreed by.
0.1	2 March 15	Initial Draft	Tom King/Stephen Laishley
0.1	27/04/2015	Policy signed off by Chief Constable – policy now live	56408 Couchman