WILTSHIRE POLICE &
POLICE AND CRIME COMMISSIONER

Acceptable Use Policy

(Force Assets, Systems, Email and Telephone)

Date of Publication: June 2021
Version: 3.0
Next Review Date: June 2023

TABLE OF CONTENTS

1. ACCEPTABLE USE POLICY STATEMENT

This policy is required to assist all Wiltshire Police Officers, Police and OPCC Staff, Special Constables, Volunteers and all contracted third parties identify what they can and cannot do when accessing Wiltshire Police/OPCC systems, and to provide clear guidance around what constitutes Law Enforcement Purposes.

This policy supports the organisations values and behaviours, in particular acting with impartiality, integrity, public service and transparency at all times.

This policy sits alongside the Microsoft Office 365 Acceptable Use Procedure which governs and provides advice on the use of Microsoft Office 365, Teams and One Note.

What is Information Security? Information security is the preservation of the confidentiality, integrity and availability of information:

a. Confidentiality - Protecting sensitive or personal information from unauthorised disclosure, both to outsiders, and to staff who have no requirement to access such information in the course of their duties;
b. Integrity - Safeguarding the accuracy and completeness of information and information processing methods;
c. Availability - Ensuring that information and associated services are available to meet the needs of the Force.

Information security is required during the entire lifecycle of a piece of information, from the moment it is collected or created, throughout its usage, through to ultimate disposal. Appropriate measures need to be applied to ensure that information security is maintained. Information security promotes trust and confidence in the Force's services, practices and IT infrastructure and systems.

The achievement of information security needs a combination of policies, standards, procedures, guidelines, appropriate organisational structure, physical security considerations, and measures to safeguard the ICT network infrastructure and information systems. This policy contains a summary of the expectations from all users of the Force's systems and applications. Where relevant, links to more detailed guidance will be provided. This Acceptable Use Policy (AUP) is part of a wider Information Security Policy Framework (ISPF) which governs the security principles that applies to the use of the Force's systems and the ISPF should be read in conjunction with this document.

APPLICABILITY

This policy is applicable to all systems and applications used by Wiltshire Police and the OPCC and applies to all Police Officers, Police and OPCC Staff, Special Constables, Volunteers and all contracted third parties, whether they are working from Wiltshire Police/OPCC premises, Shared (Partner) premises, any office, remote location, home address, or whilst working remotely.

2. ACCEPTABLE USE OF FORCE SYSTEMS

The standards of behaviour and the integrity of those who work within the police service are constantly under close scrutiny. It is imperative that Wiltshire Police Officers and Wiltshire Police/OPCC Staff conduct their business in a way which maintains public confidence. Information is provided to Wiltshire Police and the OPCC via a number of sources and there is a legal requirement that this information will be treated confidentially and only accessed for a legitimate reason: Law Enforcement Purposes or purposes covered by other policies or legal requirements.

Law Enforcement Purposes are defined as: prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Where police officers or Wiltshire Police/OPCC staff abuse their position and view confidential information without a legitimate Law Enforcement Purpose, this serves not only to undermine the trust of the public, but could also be a breach of the Data Protection Act 2018, the Computer Misuse Act 1990, the Code of Ethics, Standards of Professional Behaviour, and Force Policy.

3. GENERAL PRINCIPLES

Personnel are able to use the Wiltshire Police/OPCC IT and telephony systems for Wiltshire Police and OPCC 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 by adhering to the Code of Ethics, the Standards of Professional Behaviour;
- 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 for non-work related issues during working time, except during refreshment or other authorised breaks.

Permission to use the systems for personal use may be withdrawn if personal use adversely affects official use. This will be determined by Line Managers measured against any adverse impact on official use.

4. ROLES AND RESPONSIBILITIES

The Force Information Security Policy Framework (ISPF) contains detailed information of the various role and responsibilities that are associated with the management of information security within the Force.

5. ACCEPTABLE USE OF ASSETS

All IT devices to be used in connection with the Wiltshire Police/OPCC information must be formally configured and authorised by the ICT Department and approved by relevant information asset owners or line managers before use.

Staff must follow the Agile Working and Mobile Computing Policy and must not use personally owned (e.g. bring your own devices) electronic devices to process the Force's information or process force Information on non-police endorsed systems or software.

All of the ICT equipment and software that you have been assigned remains the property of the Force/OPCC. You have an obligation to ensure that this equipment and software is safeguarded and only used as intended:

a) You must not remove any ICT equipment from the Force's premises without Line Managers approval;
b) You must always take care of ICT equipment allocated for your use, and treat it as if it is your own;
c) You must protect your ICT equipment against theft and unauthorised access;
d) Where at all possible, you must not expose your IT equipment to any environmental hazard, such as extremes of temperature;
e) You must not install any software or attempt to use any USB device that has not been authorised by the ICT Department. If you require any software or other devices for your work, you must consult your line manager and the ICT Department;
f) You must not modify your IT equipment in any way; this includes any amendments to the hardware and software configuration;
g) You must always report any IT problems to the ICT Service Desk.

6. USER IDENTIFICATION, ACCESS AND MONITORING

You must only access and use the Police/OPCC IT network, systems and applications if you are authorised to do so. If you are granted access, it is so that you are able to perform your duties efficiently.

You must remember that access has been granted for your sole use by means of a unique user account and password. This applies to the different user accounts that may be granted to you for access to the Police/OPCC network, information systems and applications.

You must not give details of your user account and password to anyone, including your line manager; you must not share any user account allocated to you with anyone else. Wiltshire Police and OPCC (within its legal rights) is able to track the activities of each user via their user account, and identify exactly what they have accessed and what actions have been taken. If it is your user account that is logged as attempting an unauthorised or illegal action, you may be held responsible. It is in your interests to ensure that you safeguard your user account and password details at all times.

In order to ensure compliance with legislation, regulations, contracts and its information security policies, the Force reserves the right to monitor user activities.

7. INFORMATION CLASSIFICATION, LABELLING AND HANDLING

The Force's Information Classification and Handling Policy provides you with the guidance you require to be able to do your job in a secure and responsible manner. The Information Management Policy applies to all information irrespective of its form, including electronic information, e.g. databases and files, computer media based information, e.g. stored on CDs, DVDs and USB devices, and paper based documents.

All information that is handled by the Wiltshire Police and OPCC has a classification to determine the level of security it requires and the way in which it must be handled.

For every document you produce, you are personally responsible for defining its classification on behalf of the Force. When you are classifying information, you must consider its sensitivity and how much protection it needs.

Appropriate safeguards must be put in place to protect personal, sensitive and/or information classified under the Government Security Classification Scheme (GSC) (see Government Security Classification Guidance Handout for details). The extent of the safeguards should be in proportion to the degree of risk posed.

When using the Wiltshire Police and OPCC information, you must handle it in a secure manner based upon its classification.

8. SECURE HANDLING OF MEDIA AND DOCUMENTATION

Care must be taken to protect all documentation and computer media, e.g. DVDs, CDs and USB storage devices, containing sensitive and critical information, and measures must be taken to ensure secure storage, transit, copying, reuse and disposal of computer media and documentation.

When exchanging information within the Force or between other Forces/trusted organisations, it is vital to assess the sensitivity of the information and handle it in accordance with any security classification and handling requirements and the Force's Information Management Policy.

When dealing with hard copy documents, always ensure that you are aware of their security classification and handling requirements. Sensitive documents should not be left unattended on desks, printers and other equipment where they are vulnerable to unauthorised access and theft.

You must always lock sensitive computer media and documents away when left unattended.

With the global messaging opportunities presented by Internet based email, users are specifically reminded that they must adhere to the Data Protection Act 2018 and UK General Data Protection Regulations (UK-GDPR) when transferring/sending personal data to a country or territory outside the European Economic Area.

Personal data shall not be transmitted to a country or territory outside the UK 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 Data Protection Officer should be contacted if further information is required.

9. DATA PROTECTION LEGISLATION AND PRIVACY OF PERSONAL INFORMATION

All Wiltshire Police officers/police and OPCC staff and 3rd parties must have a clear understanding of their personal responsibilities under the data protection legislation and how this affects the processing of personal data. Reference should be made to the Data Protection Policy.

Wiltshire Police and OPCC will take criminal and/or disciplinary action against any category of person mentioned above who wilfully, without authority or defined policing purpose or other statutory or business purpose, accesses and/or misuses personal data held by either the Force or PCC. Any use of personal data that does not have a defined policing or other statutory or business purpose is likely to constitute a misuse.

10. COMPUTER MISUSE LEGISLATION

All users must comply with the Computer Misuse Act 1990. The Computer Misuse Act, generally aimed at computer 'hacking', specifies offences for any unauthorised access to internal organisational systems. The Act introduces three basic criminal acts:

- Unauthorised access;
- Unauthorised access with intent to commit a further serious offence;
- Unauthorised modification of computer material.

Staff (and other authorised users) must only access systems they are authorised to use. It is an offence to knowingly gain unauthorised access to a computer system, and this could result in a fine or imprisonment.

11. SITE SECURITY

Physical security involves protecting Wiltshire Police & OPCC premises, staff, information and ICT assets from unauthorised physical access and physical security threats, e.g. fire and wilful damage. All Wiltshire Police & OPCC staff must support site security requirements and adhere to the Physical Security Policy.

12. REMOVAL OF PROPERTY AND SECURITY OF EQUIPMENT OFF-PREMISES

All staff are responsible for protecting authorised off-site equipment (allocated to them) against physical security threats and unauthorised access. Staff must also ensure that off-site Force information is securely handled in line with the Force's Information Management Policy.

13. PASSWORD SECURITY

Passwords are a key control to maintain information security. They help ensure that only authorised persons have access to the Force's IT network and systems.

Passwords **MUST NOT** be easily identifiable/guessable or contain personal information that could be easily identified by hackers (e.g. names, dates, sports teams, pet names, vehicle registration numbers). In order for your password to be effective and remain secure, you must comply with the Password Policy which details the length and composition requirements for Force passwords.

You should avoid writing your passwords down, whether it's in your mobile phone or on a post-it note. It might seem like a helpful way to remember them, but if they get into the wrong hands it could put you and your account at risk. This is even more important when working from home as the risks are greater in the family home, for example they could be seen by family members or stolen in a burglary.

14. CLEAR DESK AND CLEAR SCREEN POLICY

Measures must be taken to adequately protect against unauthorised physical access to the Police and OPCC information hosted on PCs, laptops, handheld devices (e.g. tablets, mobile telephones etc.), computer media (e.g. DVDs, CDs and USB storage devices), and paper documentation. Staff must adhere to the Force's Information Management Policy and Records Management Policy.

All staff must ensure that access to their user accounts is password protected when their computer devices are left unattended, even for a small amount of time, e.g. 1 minute by locking their workstation.

All staff must ensure that all mobile equipment, e.g. laptops and tablets, sensitive computer media and sensitive documentation are not left unattended and insecure, but are appropriately stored in locked areas or facilities, e.g. locked cabinets, and that access to relevant keys is controlled.

At the end of a working day, you must:

- Logoff your PC or laptop;
- Clear your desk, and lock all sensitive computer media and documents away in a drawer or cabinet with suitably restricted access;
- If you are a user of a laptop or handheld device, and you are not taking it with you, you must lock it away in a drawer or cabinet with suitably restricted access.

15. REMOTE WORKING

Remote workers include all users who use the Force's information and information processing facilities whilst not located on the Force's premises, e.g. workers who are located in other organisations' offices, working remotely and travelling. Home workers are users who have been authorised to use the Force's information and information processing facilities whilst based at home. All remote/home working must comply with the Agile Working and Remote Computing Policy.

16. REPORTING INFORMATION SECURITY INCIDENTS

In order for Wiltshire Police and OPCC to be able to manage and deal with security incidents successfully, they must be captured and logged.

If you suspect or have knowledge of a security incident or security event, or a breach of the Force's information security policies or procedures, or a software malfunction, or a security weakness in any Force building, network or information system, you must report the concern immediately to the Information Security Officer or ICT Security Officer and/or your line manager. If out of office hours and urgent, i.e. theft of ICT device, notify the FIM immediately.
Examples of a security incident include:

- Physical damage to the Force's IT equipment;
- Compromise/loss of sensitive documents and information, e.g. personal data;
- Unauthorised use of another user's account (masquerading of user identity);

- Divulging a password to another user without authority;
- Improper use of e-mail or the Internet, e.g. harassing e-mails, downloading or distribution of pornographic images;
- Unauthorised copying of the Force's information;
- Damage to the Force's property that could impact information security;
- Access to the Force's premises without authority; and
- Theft of the Force's IT equipment.

It is vital that you report all security incidents. Withholding information and failing to report an incident could result in you being held personally liable. Staff must not attempt to deal with the security incident (other than reporting the incident). If in doubt, please contact the Information Security Officer, ICT Security Officer or your line manager for advice.

17. SECURE DISPOSAL AND RE-USE OF EQUIPMENT

All of the Force's information and software must be securely wiped from Force's IT equipment before disposal or re-use of the equipment. All equipment intended for disposal and re-use must be returned to the ICT Department who shall securely wipe Force's information and software from the equipment.

18. PROTECTION AGAINST MALICIOUS CODE

Computer viruses, spyware and other forms of malicious code exploit vulnerabilities in software programs and can cause loss and damage to the Force's and OPCC information, software and IT equipment.

Wiltshire Police and OPCC use a variety of products, e.g. anti-virus and software security patches, which are constantly updated to minimise the threat from viruses and other malicious code. PCs and laptops are also protected by these controls. You must not change or remove these controls on your Police/OPCC device, otherwise the ICT network and systems will become more vulnerable to the threat from viruses and other malicious code.

In addition to these controls, Wiltshire Police and the OPCC is also dependent on its staff, who must remain vigilant to protect it from malicious code. You must ensure that:

- You do not introduce a virus or malicious code into the Force's network, by downloading unauthorised or suspect software from the Internet or from computer media, e.g. DVDs, CDs and USB storage devices onto your PC, laptop or any Police/OPCC system;
- All software and data which originates from outside the Police or OPCC must be checked for viruses and malicious software prior to it being opened or used – if you need help, contact the ICT Helpdesk;
- If you are suspicious of a virus or malicious code, you must stop using your PC or laptop immediately and contact the ICT Helpdesk;
- If you receive a suspicious e-mail, you should not open it or the attachment or any hypertext link, as this may well activate a virus or other form of malicious code. Wiltshire Police and OPCC use an enhanced filtering system which will identify and tag 'suspect spam' emails with either SPAM or CAUTION. If you receive an email tagged with 'CAUTION' it may well be a valid email. If you feel that it is not or the email is tagged with 'SPAM' forward it to spam@wiltshire.police.uk for evaluation / confirmation.

There may also be 'hoax' virus messages in circulation which are not actually viruses at all, but plain e-mail messages asking you to take some sort of action, such as deleting files on your computer and forwarding the message. These messages themselves are not infected with a virus, and are spread by playing on people's fears, and fooling them into following the instructions. If you receive a message warning you of a virus, you must immediately contact the ICT Service Desk.

19. SECURITY EDUCATION AWARENESS & TRAINING

All personnel will receive appropriate instruction with regard to information security. At present this is covered by a mandatory NCALT MLE IM - IS training course.

20. SECURITY OPERATING PROCEDURES (SYOPS)

SyOPs, designed to assist in the efficient operation of Information Security detail the security standard against which all Information Security will be operated, define roles and responsibilities and notify users what they can and cannot do. All Users of Information Systems are required to comply with SyOPs at all times.

21. INCIDENT REPORTING

If you believe that you have accessed any record incorrectly it is your responsibility to report this to your supervisor and to make a note of the access and time it was reported. At this point, any further access of the relevant record(s) must cease.

Supervisors must then determine whether the access was necessary for Law Enforcement Purposes.

If you, as a supervisor, receive a report that any record has been accessed incorrectly (i.e. not for Law Enforcement Purposes) it is your responsibility to assess whether you believe the record was accessed incorrectly and if so, to report this to PSD or CCU.

If you believe that a colleague has accessed any record without a legitimate purpose it is your responsibility to report this to either your supervisor, PSD or CCU.

22. USE OF SPECIFIC SYSTEMS AND EQUIPMENT

22.1 Law Enforcement Applications (PNC, NICHE, Storm etc.)

The following conditions apply to the use of the Police National Computer (PNC), Police National Database (PND), NICHE, STORM, Tasking & Briefing Portal (TAB) and Force Data Search (FDS) but also applies to any other Wiltshire Police database or system.

- Any search or enquiry of PNC, NICHE, STORM, TAB or FDS must be justified as being for Law Enforcement Purposes; namely the investigation, prevention and detection of crime. This includes the legitimate accessing of information to supply to other agencies such as details of vulnerable victims or witnesses etc.
- The access must also be a part of your normal role. Conducting an enquiry in relation to a reported crime or incident clearly falls within the prevention and detection of crime.
- Researching PNC, NICHE, STORM or FDS out of curiosity, particularly where it involves looking at information regarding yourself, family, friends, acquaintances, neighbours or 'celebrities' is not permitted in **any** circumstances.
- If you believe you have a legitimate Law Enforcement Purpose to access details of a relative or acquaintance, then you must seek **prior** approval from a supervisor who will make a record of your request and make a decision as to whether it is appropriate for you to continue. You should also make a record of this request and the decision reached by your supervisor. Remember it is your responsibility to maintain your integrity.
- If you inadvertently accessed information regarding a relation or acquaintance, you have not done anything wrong, but you must cease any further research and draw this to the attention of a supervisor who may authorise your continued use providing it is for a Law Enforcement Purpose or ask for another officer or colleague to conduct the research. You should also make a record of this request, and the decision made by your supervisor.

- It is accepted that Local Crime Investigators may take an initial look at custody records relating to their assigned area at the start of their shift. This is in order to ascertain what work may be allocated to them and to assist them in organising workload priorities. Accessing custody records beyond the minimum to ascertain allocation (unless that record has been allocated to that LCI) is not permitted without prior approval from a supervisor who will make a record of that approval detailing why it is appropriate for the LCI to continue. The LCI should also make a record of this request, and the decision made by the supervisor.
- If you are a Reporting Person or Victim accessing any record on a force system (e.g. PNC, Niche RMS, Storm, FDS etc.) containing information relating to that report or incident is not permitted. If you inadvertently access information regarding or relating to that report or incident you must cease any further research, make a record of what has occurred and inform your supervisor immediately.
- Where you are a Reporting Person or Victim and a witness statement is required, it should be obtained by Investigating Officers. If you create a self-written statement it should be submitted to the Investigating Officer. Under no circumstances should you attach a statement, exhibit or any other document to the investigation.
- Where supervisors are approached to authorise a search of a Data System, the supervisor must make a considered decision as to whether it is appropriate for the staff member to continue with their enquiry. If necessary they should seek advice from CCU or PSD. A record must be made of the decision taken by the supervisor and the member of staff.
- If you are asked to search any confidential system on behalf of someone else you need to make a record of the request. This is to ensure that you can respond adequately to any later question regarding the justification for the search.

All records of requests should be made in a Pocket Note Book (PNB), or some other suitable auditable system, so that if necessary it can be produced at a later date. See Pocket Notebooks and Other Notebooks Procedure.

22.2 E-Mail/Messaging Security and Secure Internet Access

E-mail and the Internet are provided to you as a means of improving your communications, knowledge and effectiveness at work. Wiltshire Police/OPCC e-mail and Internet facilities are intended for business use, although limited personal use may be permitted, subject to approval by your line manager. Regardless, all usage of e-mail and Internet facilities is treated as the property of the Wiltshire Police/OPCC and must not be regarded as private.

All staff must be aware that the Wiltshire Police and OPCC reserves the right to use monitoring tools to enforce Force policies and to produce periodic reports detailing use of its e-mail and Internet access facilities.

Use of e-mail and Internet access introduces security threats such as malicious code attacks, e.g. viruses, unsolicited or undesirable e-mail, fraudulent attempts to acquire sensitive information such as passwords, police matters, unauthorised content, and breaches of legislation, e.g. computer misuse and copyright legislation. If you accidentally access any material which is not permitted, you must report this to your line manager and the ICT Service Desk immediately.

E-mail is an insecure method of communication and messages may well be read by those who have no authority to do so. Before sending information via e-mail, you must first assess the classification and handling requirements of that information as detailed in the Government Security Classification Scheme (GSC) (see Government Security Classification Guidance Handout for details).

The following guidelines should be considered when using e-mail, the Internet and social media applications:

- Obtain confirmation of receipt of important e-mails, particularly those containing personal data;
- Wherever possible 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;
- The sending of whole force email must be approved by an authorised person
- Be mindful of the lines between professional and private/personal matters and the importance of keeping these separate;
- Remember that emails are records and any content containing personal opinion should be professional. Emails can be retrieved and discussed and you could be identified as the author of said opinion;
- When on annual leave or away from the office for a substantial period, the “Out of Office Assistant‟ should be activated. OOO messages should be succinct and should not include information detailing the reason for physical absence, duration of absence, your job title, contact information or detailed alternative contact information. Consider having one message for internal use and one for external use (see Mailbox Management Procedure).
- It is not acceptable to send emails to personal email accounts or home computers that relate to Wiltshire Police the OPCC or criminal investigations. The use of Wiltshire Police email and social media accounts should be for work purposes only;
- Regularly weed e-mail folders to ensure messages and attachments are retained no longer than necessary in line with the Mailbox Management Procedure;
- Ensure outgoing e-mail is accurately addressed;
- Unless authorised, software must not be downloaded and you must not access or use on-line computer games;
- You must not download or copy material in breach of copyright licensing;
- You must not seek, retrieve, display or download data in any format which is indecent, offensive, subversive, illegal or otherwise inappropriate and inconsistent with Force Professional Standards;
- It is not acceptable to register Force email addresses or telephone numbers with commercial websites for personal purposes;
- You must not transmit unencrypted information classified Official-Sensitive or above over the Internet, unless in line with the Government Security Classification Scheme (GSC) and the Force’s Information Management Policy;
- Excessive personal use of Internet browsing or email messaging facilities is not permitted. (To be determined by Line Managers measured against any adverse impact on official use).

The above points relating to e-mail are also applicable to mobile applications and SMS messaging. Mobile applications must not be used to communicate Police/OPCC information unless these have been approved by the ICT Department.

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

Advice and Guidance on the use of Social Networking Sites will be issued from time to time and can be found in the Force Social Media Policy.

22.3 Information Security in Conversations and with the Use of (Mobile and Fixed) Telephone and recording Equipment

Due care must be taken when using telephones, voicemail, answering machines, facsimiles and recording equipment (e.g. photographic, video and audio equipment) to ensure the protection of sensitive information. All telephone users must be aware that any speech over the telephone is at risk of interception by unauthorised persons or groups. All staff must comply with the Force's Information Management Policy and Data Protection Policy.

It is important that before you conduct a telephone conversation in an open plan office area or outside of the Force's premises, you must consider the nature of the topic you are about to discuss. If the conversation is of a sensitive nature, you must ensure that there is no possibility of eavesdropping. Remember to always be aware of who is around you when holding a confidential conversation. In addition, messages containing sensitive Policing information must not be left on voicemail and answering machines.

When sending or receiving sensitive information by facsimile, you must ensure that the information is not compromised. Always check the recipient facsimile number to ensure that it is correct before sending information. Ensure that the information is collected immediately from the facsimile. Ensure that all sensitive information sent by facsimile is destroyed when no longer needed.

With regard to mobile phones, the following measures must be adopted:

- The business use of mobile phones is regulated in line with this policy and the Wiltshire Police Force Laptop, Tablet and Mobile Phone Acceptable Use Agreement;
- Force issued mobile phones are provided for Wiltshire Police and OPCC business use. Excessive personal use of Force mobile phones is not permitted (to be determined by Line Managers measured against any adverse impact on official use);
- Telephones should not be left unattended and insecure;
- Mobile Phones unused for 90 days will be wiped. If the mobile phone is still required following this provision the officer/member of staff must request a new phone;
- Telephones should not be used for sensitive conversations. Where practicable, work and personal mobile telephones are forbidden from areas where highly sensitive information is discussed on a regular basis.

22.4 Airwave Radios

The conditions of use for Airwave radios is detailed in the Airwave Security Operating Procedure (SyOPs). No departure from or amendment to the SyOPs is permitted.

All authorised users of Airwave radios have a personal responsibility for the preservation of the confidentiality, integrity and availability of information and information / communications systems / devices entrusted to them.

Once issued, whether on a long or short-term basis, users of Airwave radios become directly responsible for the for the physical security of the radio and any ancillary equipment. Equipment loss / compromise has the potential to endanger Wiltshire Police communications and the communications of other Airwave Service subscribers.

22.4.1 User Responsibilities

Once issued with an Airwave Radio, the following key responsibilities are transferred:

- In the event of a radio being lost, stolen or showing evidence of tampering, it must be reported as soon as is practicable to the Divisional Radio Custodian, or out of normal duty hours, to the Force Critical Incident Manager or Force Operations Room Supervisor. In addition to this, a 232 report must be submitted to Line Manager outlining the exact circumstances of the loss for further investigation.
- Holders must ensure that when the radio is not in use it is powered down, returned to secure storage at the end of each duty period, never left unattended and if unserviceable, returned directly to the Divisional Radio Custodian.
- Annual audits will be conducted on all personally issued radios and when requested to do so, holders must confirm they are still in possession of the asset. Failure to do so may result in the radio being disabled on the network as a security precaution.

22.4.2 Supervisory Responsibilities

Supervisors and managers have a responsibility for ensuring all authorised users of Airwave Services comply with Infosec and other complementary policies and procedures. A proactive approach should be taken to ensure compliance with SyOPs including reporting actual or suspected instances of non-compliance or other breaches of security.

Supervisors are responsible for the security and oversight of the Temporary Pool booking out process. The key to the Temporary Pool radio cabinet must be kept secure at all times and only accessible to authorised personnel.

23. ACCESS CONTROL LEVEL (ACL) OF NICHE AND OTHER RECORDS

Restricting access to Police databases may cause potential risk to individuals and the organisation as previous history and intelligence may not be visible to parts of the workforce. The request to restrict records will therefore need to be justified with a documented rationale balanced against the requirement to protect the integrity of an investigation.

For guidance on the application/review/removal of ACL please refer to the Procedural Guide to the Application / Review / Removal of Access Control List (ACL) in NICHE RMS.

23.1 Authorisation to Apply ACL

Authorisation to ACL a Niche record or entry on another type of database is to be authorised by the Senior Investigating Officer (Inspector / Police Staff equivalent or above). Such authorisation will only be given when certain circumstances apply. These will be as follows:

- A record relating to a matter which is currently subject of a covert policing operation;
- A record relating to a criminal offence where a member of a UK police force, (officer or staff) are implicated as a suspect and are currently subject of a criminal investigation;
- Exceptional circumstances – What constitutes an exceptional circumstance will be judged on a case by case basis by the SIO considering authorisation of ACL, but would need to be more serious and sensitive than the above.

23.2 ACL Reviews

It is the responsibility of the supervisor responsible for an investigation to review the decision and rationale for the ACL in line with the Hierarchical Crime Review Procedure. If the ACL is still required the rationale for continuing the ACL must be recorded on the Occurrence Enquiry Log (investigation log).

If the ACL is no longer required the supervisor must notify CCU who will inform the Data Quality Team (DQT) accordingly.

On closing an occurrence the supervisor must ensure that the ACL is removed by notifying CCU who will inform DQT accordingly (See Access Control Lists (ACL) in Niche RMS Procedural Guide).

23.3 ACL For Intelligence

For information on authorizing the use of intelligence ACLs, understanding the hierarchy of access to intelligence between departments, auditing access to ensure information security and the process for review and removal of intelligence ACLs please refer to the Access Control Lists (ACL) for Intelligence Policy.

24. MONITORING, INTERCEPTION AND AUDIT

Wiltshire Police and OPCC reserves the right to monitor all communications (including telecommunications) using Force communications systems and where appropriate inspect the content of Email transmissions, text messages, Internet browsing sessions and smartphone application use. Such activity is considered necessary for the purposes of:

- Protecting the network from malicious software, denial of service attacks and other external threats;
- To investigate or detect use of computers contrary to legislation, policy or procedure;
- 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;
- In the interests of national security.

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

The Investigatory Powers Act 2016 (IPA) establishes a basic principle that communications may not be intercepted without consent and ensures compliance with ECHR and fundamental freedoms.
The Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018 make an exception to IPA and allow businesses (including public authorities) to intercept communications transmitted across their systems without consent for certain purposes.

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

- to ascertain compliance with regulatory or self-regulatory practices or procedures;
- for an appropriate method of ascertaining standards;
- to prevent or detect crime;
- to investigate or detect unauthorised use.

Wiltshire Police Counter Corruption Unit is authorised to carry out the appropriate auditing of system use.

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

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.

In all cases, regulations require the Force to make all reasonable efforts to inform every person using or who may use the system that interception, monitoring and auditing 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, communications & messaging applications and E-mail) may be intercepted, 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.

25. BREACH OF POLICY ESCALATION PROCEDURES

25.1 Purpose of Procedures

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 Police Regulations or Police Staff Discipline Procedure.**

25.2 Roles and Responsibilities

The Counter Corruption Unit is responsible for conducting activity and audit of Force information systems and stored data. The ICT Department will provide technical assistance as appropriate for activities requiring additional technical support.

Potential policy breaches discovered by ICT Department staff during normal system administration must be reported to the Head of Information Management and Assurance in the first instance.

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

The Chief Constable has authorised the Professional Standards Department to undertake routine Intelligence lead and random audit of Force systems to ensure that appropriate and proportionate compliance is in place.

Requests for specific additional audit of activity of an individual member of staff's use of Force systems must be made through formal application (Form 840).

Before the Counter Corruption Unit undertake specific auditing requests they must be authorised by the Head of the Counter Corruption Unit. Audits concerning the recovery and review of stored/Archived data are not subject to provisions under The Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018. See Para 2 for Monitoring and Intercept provisions and authority level.

The results of audits 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.

25.3 Records

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

26. AUTOMATED RESTRICTIONS

To enable the Head of ICT 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.

POLICY AIM

The primary aim of this policy is to set out the rules and conditions regulating the use of Wiltshire Police and OPCC systems including the use of the Police/OPCC telephone network and issued mobile telephones.

In keeping with the objectives to inspire public confidence in the Forces ability to protect the confidentiality, integrity and availability 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 Wiltshire Police/OPCC information security policy documents.

LEGAL BASIS AND DRIVING FORCE

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 2018 / UK General Data Protection Regulations (UK-GDPR)
- 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)
- Investigatory Powers Act 2016
- The Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018

RELATED POLICIES, PROCEDURES and OTHER DOCUMENTS

Access Control Lists (ACL) for Intelligence Policy
Agile Working and Mobile Computing Policy
Government Security Classification Guidance Handout
Hierarchical Crime Review Procedure
Information Management Policy
Information Security Policy Framework (ISPF)
Microsoft Teams Meetings Recordings Acceptable Use Procedure
Password Policy
Physical Security Policy
Pocket Notebooks and Other Notebooks Procedure
Procedural Guide to the Application / Review / Removal of Access Control List (ACL) in NICHE RMS
Records Management Policy
Records Retention Schedule
Social Media Policy

AUTHORISED PROFESSIONAL PRACTICE

Professional Standards
Information Management

DATA PROTECTION

Any information relating to an identified or identifiable living individual recorded as a consequence of this policy will be processed in accordance with the Data Protection Act 2018, General Data Protection Regulations and the Force Data Protection Policy.

FREEDOM OF INFORMATION ACT 2000

This document has been assessed as suitable for public release.

MONITORING AND REVIEW OF THIS POLICY

The Head of Information Management and Assurance will ensure that this policy is reviewed every two years.

Regular proactive and reactive audits together with analysis of staff misconduct trends will be conducted by the Professional Standards Department to establish compliance with this policy. Non-compliance will be reflected in future policy reviews.

WHO TO CONTACT ABOUT THIS POLICY

The Head of Information Management and Assurance for this policy.

All queries relating to this policy should be directed to the Information Security Officer or the Force Policy Officer.

DOCUMENT ADMINISTRATION

Ownership:

Department Responsible: Information Management and Assurance
Policy Owner/Author: Keith LEWIS / NCC Group
Technical Author: Neil COWLING, Andrew IRVING
Senior Officer/Manager Sponsor: Deputy Chief Constable

Revision History

Revision Date	Version	Summary of Changes
07.06.2021	3.0	Policy rewritten as part of the NEP. Text on: User identification, information classification, secure handling, Data Protection, site security, removal of property & security of equipment, password security, clear desk policy, remote working, reporting information security incidents, use of specific systems (including PNC, Niche, Email Telephone, mobiles & Airwave), ACL, monitoring interception and audit, breach of policy escalation and automated restictions added.
17.03.2022	3.0	Section 22.2: requirement for emails relating to on-going Inquiries into Child Sexual Abuse / Undercover Policing to be retained removed.

Approvals

This document requires the following approvals:

Name & Title	Date of Approval	Version
Continuous Improvement Team	07.06.2021	3.0
JNCC (via email)	07.06.2021	3.0

Distribution

This document has been distributed via:

Name & Title	Date of Issue	Version
E-Brief		
Email to relevant affected Staff/Officers		

Equality Impact Assessment

Has an EIA been completed? If no, please indicate the date by which it will be completed. If yes, please send a copy of the EIA with the policy.	☒**Yes** ☐**No** **Date**:

Consultation

List below who you have consulted with on this policy (incl. committees, groups, etc.):

Name & Title	Date Consulted	Version
Keith LEWIS, Mark LEVITT, Laura NORTH, Neil COWLING, Jonathon JONES, Matt GIRDLESTONE	11.03.2021	0.8
Police Federation	16.02.2021	0.8
UNISON	03.02.2021	0.8

Implications of the Policy

Training Requirements

There are no additional training requirements for the implementation of this Policy.

IT Infrastructure

No new IT infrastructure is required for the implementation of this Policy.