WILTSHIRE POLICE &
POLICE AND CRIME COMMISSIONER

Agile Working and Mobile Computing Policy

Date of Publication: December 2021
Version: 2.0
Next Review Date: December 2023

TABLE OF CONTENTS

SCOPE

This Policy applies to all Police Officers, Police and OPCC Staff, Special Constables, Volunteers, and employees from external agencies or organisations who by the nature of their role, are required to access Wiltshire Police/OPCC information and information assets using mobile devices.

The devices in scope of this policy include all corporately owned / formally approved end use devices used to remotely access Wiltshire Police & OPCC resources or used for any other work related purpose. This document contains responsibilities and guidance for the following subject areas related to these mobile devices:

- User Responsibilities
- Agile Working
- Mobile Device Registration
- Device Requirements
- Data Requirements
- Data Backup
- Monitoring
- Device Resetting and Agile Wiping
- Termination of Contract

This policy operates alongside the Acceptable Use of Force Systems Policy and the HR Agile Working Guidance.

INTRODUCTION

The objective of information security is to ensure all information is always reliably and securely authorised and authenticated; that it cannot be corrupted or disclosed to unauthorised persons and its origin is authenticated. It is the policy of Wiltshire Police and the OPCC to ensure that information, networks, systems, applications and equipment are protected from all threats, whether internal or external, deliberate or accidental. A key part of the policy, therefore, requires that mobile devices are secured and access to Wiltshire Police and OPCC resources via portable computing end user devices is secured.

POLICY STATEMENT

The policy of Wiltshire Police and the OPCC regarding portable computing end user devices is as follows:

- All access to Wiltshire Police and OPCC resources via mobile devices will be in accordance with the minimum privilege principle in that access is denied, except where it is specifically required for legitimate purposes
- All portable computing end user devices must be adequately secured to prevent theft
- All Wiltshire Police and OPCC personnel will be accountable for their actions using portable computing end user devices to access Wiltshire Police and OPCC resources
- Only approved and authorised portable computing end user devices, using Wiltshire Police mobile device management solution, are to be used to access Wiltshire Police and OPCC resources
- Storage of data on mobile devices must be minimised to what is necessary and all data must be handled in accordance with the Records Management Policy and Information Management Policy
- Users must report all lost, stolen or compromised devices immediately to the ICT Helpdesk or the FIM via CCC if out of office hours

- Users must notify the Data Protection Officer of any known or suspected personal data breach by completing a Data Breach Reporting Form as soon as is practicable (and within 72 hours) of the breach
- All portable computing end user devices must be used in line with all Wiltshire Police and OPCC policies

RESPONSIBILITIES

All Wiltshire Police and OPCC personnel using portable computing end user devices to access Police and OPCC resources have a responsibility to adhere to this policy.

Wiltshire Police Information Management and Assurance Department has direct responsibility for maintaining this policy and, along with Human Resources and Health & Safety, providing advice on implementation.

Line Managers

Line managers are responsible for assessing individuals under their supervision for suitability for agile working and for regularly reviewing that suitability in line with Force/OPCC requirements. An individual's suitability will depend on the type of role and work to which they have been assigned.

Managers have an absolute discretion to authorise and withdraw agile working from a member of staff; any decision of the line manger regarding agile working must be based on sound business or performance reasons. Normal procedure in terms of performance will be followed and a decision may be taken to whether the work style is appropriate or conducive to assisting the individual in improving their performance.

Agile Workers

Agile workers are employees who can undertake work at alternative locations and are enabled to work at the most effective location to do their job. This includes Wiltshire Police and OPCC staff located in other organisations' offices, at hotels and conferences, travelling workers, working from Police vehicles, and workers who have been authorised to work from home.

All policies and procedures that apply to staff based at Wiltshire Police offices also apply to agile workers.

All Wiltshire Police/OPCC agile workers must be available and contactable during agreed working hours and are expected to continue to attend meetings and attend office locations as required.

Line Managers have the right to request that agile workers attend their usual workplace on day(s) and time(s) to suit both the manager and member of staff and to request general updates on service activities or progress towards objectives/targets or for other reasons connected to the staff members role requirements. Any such request should provide as much notice as possible that attendance is required.

Electronic diaries are to be used at all times and must be open for colleagues to view. Staff must ensure that their contact details are up to date including the publication of Force issued mobile phone numbers.

AGILE WORKING

[NB: This section must be read in conjunction with the Wiltshire Police / Wiltshire and Swindon OPCC – Agile working guidance.

General

By using Wiltshire Police and OPCC portable computing end user devices, users agree to take reasonable steps to protect Wiltshire Police and OPCC data stored on, or accessed, by those device. These steps include, but are not limited to:

- Doing what is necessary to ensure the adequate physical security of the device
- Ensuring the device's security controls are not subverted via security software changes and/or security setting changes
- Reporting a lost, stolen or compromised device immediately to the ICT Helpdesk or the FIM via CCC if out of office hours

Personally Owned Devices

Staff must not use personally owned (e.g. bring your own devices) electronic devices or software to process Force information.

Wiltshire Police and OPCC Devices

For all devices that are centrally managed by Wiltshire Police and the OPCC, the user is responsible for using the device in accordance with the Acceptable Use of Force Systems Policy and other applicable Wiltshire Police/OPCC policies.

Physical Security

The following measures are required to reduce the risk of physical security threats to mobile and home working computer devices and Wiltshire Police/OPCC information:

- Portable computing end user devices shall never be left unattended and unprotected when in a public space
- A clear screen Policy shall be implemented and when left unattended ICT equipment shall be logged-off or secured by a password-protected screen saver by pressing the Ctrl-Alt-Delete buttons and selecting the 'Lock Computer' option
- Where possible computer equipment ~~shall~~ should not be positioned or left so that it can be easily seen by members of the public, whilst working at home or non police premises (e.g. through ground floor windows)
- Computer screens shall be positioned so that information cannot be overlooked by fellow travellers, co-residents of the premises, family, visitors, or any other unauthorised person
- Smart devices (such as Apple's Siri, Amazon Echo, Google Home, Apple Homepod, Facebook Portal) should be turned off to avoid any accidental or intentional listening or recording of conversations
- Family members, friends, visitors or anyone else shall not use equipment and sensitive information
- A clear desk Policy shall be implemented and all Wiltshire Police/OPCC documentation, files (including any paper notes and notebooks), and removable computer media e.g. USB, CDs and DVDs should be stored securely and out of sight when left unattended. Removable media should be removed from computers when not in use
- You should be aware of and take into consideration the Government Security Classification (GSC) of the information that you are working on; are the security considerations appropriate?
- Printing from home from non Wiltshire Police printers is forbidden. Work related information should be kept in a digital format only. If there is a need to print anything it is expected that staff working remotely will use printers at Wiltshire Police and OPCC facilities or printers supplied by ICT

- Any printed documents must be handled and stored securely until they can be disposed of using Force confidential waste bins or shredders. Do not use home shredders and never dispose of documents alongside home recycling or waste
- When transporting mobile devices by road, rail etc. at no time shall the device be left unattended. Mobile devices can be locked away out of sight if unobserved by strangers, but shall not be left, e.g. in a car, for long periods of time or overnight
- Each unit / department must record files being taken home, and their subsequent return.
- Users must report all lost, stolen or compromised devices immediately to the ICT Helpdesk or the FIM via CCC if out of office hours
- Users must notify the Data Protection Officer of any known or suspected data breach by completing a Data Breach Reporting Form as soon as is practicable (and within 72 hours) of the breach
- Mobile devices shall be carried as hand luggage when traveling and kept within sight and reach at all times, including at airport security checkpoints;
- No Force mobile device can be taken outside the European Economic Area (plus Switzerland) without the permission of the Head of Information Management & Assurance PSD. Certain countries have specific restrictions on the use of encrypted technology that could lead to equipment being seized

Health & Safety

Under the Health and Safety at Work Act an employer has to take reasonable steps to protect the health, safety and welfare of its staff. There is a duty to carry out risk assessment in relation to work activities for all staff.

This does not mean that it will be necessary to visit the homes of every member of staff who carry out some percentage of their work at home. However, staff are required to familiarise themselves with the potential hazards. Staff are prohibited from taking hazardous substances from the work place to home.

For occasional work from home Wiltshire Police and OPCC employees will be responsible for completing their own workstation assessment on their home work station. Police and OPCC staff are responsible for ensuring a safe working environment is established and maintained whilst working from home or other non Wiltshire Police premises. See Display Screen Equipment Procedure.

It is not considered appropriate to combine home-based working with caring for dependants. Employees must be made aware that working from home is not a substitute for making arrangements for care of dependants but can provide greater flexibility.

Staff are responsible for the safety of the wiring/electricity circuit in their homes. In addition, it is important to ensure that any electrical equipment, for example laptop computers provided for work at home, is safe and regularly maintained and employees should bring in such equipment for checking in accordance with Faculty/Service maintenance agreements and should also ensure that any personal equipment used is also maintained regularly.

Legal Implications – working from home.

Working from home is perfectly legal and will not affect your residential council tax or the VAT on fuel bills. Equipment provided and owned by Wiltshire Police is covered by Wiltshire Police and OPCC insurance provided reasonable care is taken to protect it. Staff will be responsible for any loss arising from misuse, abuse, wilful damage or negligence relating to Force equipment in their care. Any loss or damage to force equipment should be reported immediately to the ICT Helpdesk or the FIM via CCC if out of office hours.

Individual contracts, agreements and employee terms and conditions, including shift patterns or core hours, will not change as a result of mobile working. Current force procedures, such as Flexible Working, and contractual arrangements will continue as normal.

ACCESS REGISTRATION REQUIREMENTS

All mobile device users must:

- Install the Wiltshire Police Mobile Device Management (MDM) solution on the device (this will be provided by the ICT Helpdesk)
- Agree to the device reset and data deletion requirements
- Not give or lend the mobile device to any person not authorised by Wiltshire Police

DEVICE REQUIREMENTS

General

As per the requirements enforced by the MDM solution, all mobile devices, as relevant, must:

- Be running the latest operating systems as required by the MDM solution
- Have remote wipe enabled
- Have disk or file encryption enabled

The ICT Department will ensure all of the above prior to user registration.

Passwords

All mobile devices must require a password to be entered to access the device. Passwords must be selected in accordance with the Password Policy.

Protection Against Malware

The ICT Department must ensure there is adequate protection against malware. For devices that are particularly susceptible, this will mean installing and running an anti-virus application on the device.

DATA REQUIREMENTS

All Wiltshire Police and OPCC data must remain stored within the applications managed by the Wiltshire Police MDM solution.

DATA BACKUP

Backup of Wiltshire Police and OPCC data to locations that are not managed by Wiltshire Police or the OPCC is not permitted.

Backup and recovery procedures and technology are implemented for centrally held data to protect Wiltshire Police and OPCC from losses or corruption of information and software (e.g. due to unauthorised changes to information and software, technical failures, malware and fire).

All personnel are responsible for ensuring that any data that they create or change is backed up on a regular basis. This is achieved by ensuring that data is stored on the central systems that Wiltshire Police/OPCC provides.

All corporate devices will be configured so that automatic backup of Wiltshire Police and OPCC data to unauthorised locations is disabled. All personnel must ensure these configurations are not changed and that work related data is being backed up onto Wiltshire Police/OPCC approved systems.

MONITORING AND PROTECTION

In order to ensure the security of Wiltshire Police/OPCC information is maintained, Wiltshire Police and OPCC reserves the right to:

- Monitor Wiltshire Police/OPCC resources, including Wiltshire Police/OPCC data residing on a mobile device, where in line with local laws and regulations
- Modify, including remote wipe or reset to factory default, a registered mobile device
- Conduct checks of device configuration to ensure compliance with all applicable policies

DEVICE RESET AND DATA DELETION

By using mobile devices for work, and therefore using the MDM solution, all Wiltshire Police and OPCC personnel accept that Wiltshire Police/OPCC data on the device will be remotely wiped under the following circumstances:

- The device is lost, stolen or believed to be compromised
- The device is found to be non-compliant with this policy
- Device inspection is not granted in accordance with this policy
- The device belongs to a user that no longer has a working relationship with Wiltshire Police or OPCC
- The user decides to uninstall the Wiltshire Police MDM solution

TERMINATION

Upon termination of the contract between Wiltshire Police or the OPCC and a mobile device user, the user must delete all Wiltshire Police/OPCC data on all mobile devices prior to termination, after the data has been centrally backed up to Wiltshire Police/OPCC systems; if this is not possible, the user must present the device(s) to the ICT Department for such deletion to occur. Where possible, the device will be reset to factory defaults.

All mobile devices and equipment held at time of resignation, transfer or retirement **MUST** be returned to ICT.

POLICY AIM

The purpose of this document is to specify and communicate security requirements to all Wiltshire Police and OPCC personnel for using and managing mobile devices that access Wiltshire Police/OPCC resources from official and remote locations.

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 designated as agile workers 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.

RELATED POLICIES, PROCEDURES and OTHER DOCUMENTS

Agile Working Guidance
Acceptable Use of Force Systems Policy
Data Protection Policy
Data Breach Procedure
Display Screen Equipment Procedure
Information Management Policy
Password Policy
Records Management Policy

AUTHORISED PROFESSIONAL PRACTICE

There are no associated Authorised Professional Practice areas at present.

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.

MONITORING AND REVIEW

This Policy will be reviewed in 2 years and at other times as dictated by organisational needs. The date of next review is December 2023.

WHO TO CONTACT ABOUT THIS POLICY

The Head of Information Management and Assurance is responsible for this policy. All queries relating to this policy should be directed to the Head of Information Management and Assurance or Force Policy Officer.

DOCUMENT ADMINISTRATION

Ownership:

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

Revision History:

Revision Date	Version	Summary of Changes
October 2021	1.7	Scheduled review: General tidy up – removal of superfluous text, clarification added around physical security and reporting of lost/stolen equipment.
December 2021	2.0	Draft v1.7 published as substantive version 2.0
January 2022	2.0	Reference to PSD removed from last bullet point page 6
March 2022	2.0	Physical Security restriction on removing mobile devices overseas changed to outside the European Economic Area (plus Switzerland).

Approvals:

This document requires the following approvals:

Name & Title	Date of Approval	Version
Force Policy Officer	15.12.2021	1.7
Keith LEWIS	23.11.2021	1.7
JNCC	13.12.2021	1.7

Distribution:

This document has been distributed via:

Name & Title	Date of Issue	Version
E-Brief		
Email to relevant affected Staff/Officers		
Other: (state method here)		

Diversity Impact Assessment:

Has a DIA been completed? If no, please indicate the date by which it will be completed. If yes, please send a copy of the DIA 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, Naji DARWISH, Suzie THOMPSON, Gemma MULLAN, Janine CHOWNEY, Laura NORTH, Sarah SOMERS	12.10.2021	1.4
UNISON, Police Federation, Jonathan JONES, Adrian HUDSON, Leonie CALLAND, Neil COWLING	12.10.2021	1.4

Implications of the Policy:

Training Requirements

None

IT Infrastructure

None