Mobile Working Policy

Wiltshire Council

Where everybody matters

Document Control

<table>
<tr><td><b>Reference Number</b></td><td><b>Version</b> 2.0</td><td><b>Status</b> Published</td><td><b>Sponsor(s)/Author(s)</b> Tim Way, Sarah Davis-Solan</td></tr>
<tr><td>Amendments</td><td colspan="3">Regular Review</td></tr>
<tr><td colspan="4"><b>Document objectives:</b> To ensure compliance with statutory requirements in relation to the handling of information outside the boundaries of Wiltshire Council premises (including working at home)</td></tr>
<tr><td colspan="4"><b>Intended Recipients:</b> Wiltshire Council Officers</td></tr>
<tr><td colspan="4">Group/Persons Consulted: None</td></tr>
<tr><td colspan="4">Monitoring Arrangements and Indicators: None</td></tr>
<tr><td colspan="4">Training/Resource Implications:</td></tr>
<tr><td colspan="2">Ratifying Body and Date Ratified</td><td colspan="2">Information Governance Programme Board September 2017</td></tr>
<tr><td colspan="2">Date of Issue</td><td colspan="2">September 2017</td></tr>
<tr><td colspan="2">Review Date</td><td colspan="2">September 2018</td></tr>
<tr><td colspan="2">Contact for Review</td><td colspan="2">Information Governance</td></tr>
<tr><td colspan="2">SIRO signature</td><td colspan="2"></td></tr>
</table>

Associated Documentation

Policies

Wiltshire Council controlled documents

- Network Security Policy
- Information security Policy
- Information Governance Policy
- Information Governance Management Framework
- Mobile Working Policy
- Information Asset Change Policy
- Information Security Policy
- Information Incident Management Policy
- Records Management Policy
- Protective Marking Scheme
- Bring your own device (BYOD) policy

Legal framework

- Data Protection Act 1998
- The Computer Misuse Act 1990
- The Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Copyright Design and Patents Act 1988

Codes of Practice and Guidance

- ISO 27000:2013 Document Series Relating to Information Security IG Toolkit https://www.igt.hscic.gov.uk
- Cyber Essentials https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
- PSN Code of Connection (CoCo) https://www.gov.uk/guidance/apply-for-a-public-services-network-psn-connection-compliance-certificate
- Government End User Device Security and Configuration Guidance https://www.gov.uk/government/collections/end-user-devices-security-guidance
- Payment Card Industry Data Security Standards PCI-DSS

Contents

1. Purpose

This policy promotes best practice for handling information outside of Wiltshire Council (the council) premises (including working at home).

The policy aims to enable and support employees intending to use and transfer manual and electronic records between the council, home and the wider community.

This policy must be used in conjunction with the Acceptable Use Policy for email, internet and computer use.

2. Scope

This policy covers the use of any mobile device, regardless of location, and applies to:

- All employees of the council, elected representatives, other workers who may not be directly employed by the council (e.g. agency workers, contractors, self-employed consultants, authorised 3rd party suppliers and duly authorised visitors);
- The physical security of IT equipment;
- The confidentiality of manual and electronic data.

Line manager authorisation must be sought by users who wish to use mobile computing facilities, either on or off-site (including at homes), or to transfer information between computer systems via physical media.

Authorisation is not required for the transfer of ‘off-site’ paper records. Paper records should be used in line with the council’s Records Management Policy.

3. Definitions

Data devices

Any device that can store data, images or other information, such as laptops, tablets, personal digital assistants (PDAs), smartphones and digital audio/visual recording/playback devices (i.e dictaphones, digital cameras and mobile phones).

Media

Any physical device which stores data, images or other information, and requires another device to access it. For example: CD, DVD, floppy disc, tape, digital storage device (flash memory cards, USB keys, portable hard drives).

Personal information

Person identifiable information can include one or more of the following:

- Name
- Address (home or business)
- Postcode
- NHS No
- Email address
- Date of birth
- Payroll number
- Driving Licence
- Bank, financial or credit card details
- Mother’s maiden name
- National Insurance number
- Tax, benefit or pension Records
- Health, adoption, employment, school, Social Services, housing records
- Child Protection
- Safeguarding Adults

Sensitive information includes:

- Racial / ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Physical or mental health
- Sexual life
- Criminal offences
- Biometrics; DNA profile, fingerprints

4. Policy Summary

Users of information will:

- Keep usage to a minimum in public areas;
- Only use information for work related purposes;
- Ensure the security of information;
- Keep equipment and files locked out of sight during transit;
- Scan any media used to transfer data for viruses using up-to-date anti-virus software;
- Ensure equipment/files are packaged in line with council guidelines during transit to prevent damage or tampering;
- Only connect council-provided or ICT-approved equipment to the council's network and/or equipment;
- Only store data on council-provided or ICT-approved equipment;
- Not send council data to personal email addresses or private internet storage sites (e.g. Dropbox, Google Drive);
- Not dispose of any media (including paper) off-site;

5. Physical Security/access control

Use of any information away from the workplace must be for authorised work purposes only.

Users must ensure the security of information from theft as well as ensuring that unauthorised individuals are not able to see information or access systems.

- All documents that contain confidential information must be appropriately secured.
- Confidential waste must be brought back to the office to be disposed of in the normal way.

Usage in any public accessible area

Mobile working in a publicly accessible area increases the risk of "overlooking" and theft. Users should keep the use of sensitive data to an absolute minimum and not leave equipment unattended at any time.

Usage in areas not generally accessible to the public (other organisational premises)

Users are responsible for ensuring that unauthorised individuals are not able to see information or access systems. If equipment is being used outside of its normal location and might be left unattended, users will need to secure it by other means.

Home Usage/Home working

Users must take steps to ensure family members or visitors are not able to access equipment or data, and equipment must be used for work purposes only.

A Clear Desk approach must be applied, where possible information should be stored in a locked container (filing cabinet, lockable briefcase). If this is not possible, when not in use it should be neatly filed and stowed away.

Supplied equipment

Council-supplied data devices, must only be used by members of staff who are authorised to do so. Deliberately or inadvertently allowing unauthorised access may result in disciplinary proceedings

The ICT Department is responsible for ensuring that supplied equipment has appropriate anti-virus software installed, and that software and firmware patches are up-to-date and the device is encrypted.

For supplied equipment which is not classed as portable, the ICT department are responsible for ensuring anti-virus software is regularly updated, software patches/firmware's/software updates are up to date and the device is encrypted. This will require the return of equipment therefore staff must return equipment for updating and checks by the ICT Department when requested.

Users should regularly connect ICT-supplied portable equipment to the council's network to allow for anti-virus software updates and software patching.

Person identifiable data files should have additional protection against unauthorised access (for example an additional password) when being transferred.

Council supplied phones and smartphones should not be used to make personal calls or send text messages. "Reasonable use" (as defined by line managers) of the internet is permitted during breaks provided is does not interfere with work or incur costs.

Loss or theft of a mobile device must be reported immediately to line management and the ICT Service Desk. The user is responsible for reporting any theft to the police to obtain a Crime Reference number, which must be given to the ICT service desk.

Users must remove data prior to returning equipment which is no longer needed.

The Council is responsible for safety testing and annual PAT testing of supplied equipment. Users must ensure the equipment is available for such testing.

Staff owned equipment - Bring Your Own Device (BYOD)

Council data and council networks must not be accessed on users' personal device unless the device has been approved for use in line with the BYOD. Users wishing to have a device approved for use should contact the ICT Service Desk.

Loss or theft of a BYOD enabled personal device be reported immediately to line management and the ICT Service Desk. The ICT Service Desk will disable the BYOD connection to the council's systems and may remotely wipe data from the device.

Guest and WiltsOnline networks should not be used for work purposes as they are not designed to protect data. These networks are segregated from the core corporate council network and are available for personal use subject to registration with ICT.

Users must ensure that data is transferred back to the appropriate network storage area, before being deleted device/media. ICT are responsible for the permanent erasure of data on devices, prior to reallocation or disposal.

Home working

Home working is defined as a member of staff whose main office is their home. Line manager authorisation must be gained prior to working at home.

Home workers must ensure:

- Any controlled document (e.g. social care record) they have will be traceable to their location and that any procedure to note the location of a file required by the organisation will be rigidly applied by them.
- Their house and content insurance covers them for the loss of any equipment provided by the employing organisation.

Any staff member who is classed as a home worker is responsible for following health and safety regulations, and undertaking a display screen equipment (DSE) assessment in line with council policies.

Users should adhere to the council's Acceptable Use Policy for email, internet and computer use when working from home.

6. Connection to the Network

Council devices may be connected to external networks which require a password. However, some public Wi-Fi networks which require further authentication (e.g. via a third-party website) may not work due to the council's security requirements.

7. Transport/storage

When users remove equipment, files and data from council premises, they are responsible for ensuring its safe transport and storage.

- Equipment should be password protected whenever possible;
- Equipment must be transported securely;
- Equipment should be stowed away securely, out of sight (e.g. in the locked boot of a car); do not leave equipment in your vehicle overnight;
- Appropriate packaging should be used to prevent physical damage to equipment or data ;
- Where data is transported or sent by non-electronic means, then council usual council guidelines apply (double envelope, etc.).

8. Disaster recovery/major incidents

In the event of a major incident or disaster, the organisation may recall all equipment on loan to provide priority functions and services.

9. Termination of Employment / Contract / Agreement

On leaving the employment of the council, all equipment, software and information must be returned.

Line managers are responsible for notifying ICT so that accounts can be closed and any BYOD access can be removed.