ABERDEENSHIRE COUNCIL

CODE OF PRACTICE: REMOTE WORKING

PURPOSE

This is Aberdeenshire Council's Code of Practice: Remote Working. This document provides guidance in plain language on information security requirements and recommendations for use of mobile computing technologies e.g. laptops, Smartphones, USB memory sticks, etc. and guidance in plain language for secure remote working.

CONTENTS

1. INTRODUCTION

This is Aberdeenshire Council's Code of Practice: Remote Working. This document provides guidance in plain language on information security requirements and recommendations for use of mobile computing technologies e.g. laptops, netbooks, tablet PCs, Smartphones, USB memory sticks, etc. and guidance in plain language for secure remote working.

This Code of Practice has been developed based on the following best practice:

- ISO17799 Code of Practice for Information Security Management – 11.7 Mobile Computing and Teleworking
- Her Majesty's Government Security Policy Framework
- CESG PSN Code of Connection
- CESG Good Practice Guide No 10 – Remote Working

1.1 Scope

This Code of Practice applies to all employees, contractors and any other individuals working with or for the Council who utilise mobile computing technologies e.g. laptops, Smartphones, USB Memory Sticks, etc. and/or who work remotely.

1.2 Review

This Code of Practice will be reviewed regularly to ensure that it remains an accurate and useful guide to secure mobile computing and remote working. The Information Management Group (IMG) is responsible for the review and the approval of changes to this Code of Practice. It is your responsibility to ensure that you remain familiar with the contents. The most up-to-date copy of this document can be found on the Information Security Home Page in Arcadia (within Our Council, Information Governance, Information Security).

1.3 Legal Precedence

For the avoidance of doubt and in the event of an apparent contradiction occurring between legislation, policy or best practice guidelines, legislation will take priority. This also applies to any future legislation that may be enacted.

1.4 Referenced Documents and Glossary

Unless otherwise stated, all documents are held in Arcadia.

1.5 Help with this Code of Practice

If you require help to apply this Code of Practice first discuss the matter with your line manager. If required please then contact the ICT Service Desk on 01224 664000 or log a call via AskFred.

2. DEFINITIONS

2.1 Portable Electronic Device (PED)

A portable device with the ability to store, process or transmit information.

A PED may be one of, or a functional combination of:

- Laptop, Netbook or Tablet device
- Personal Digital Assistant (PDA), Smartphone or Mobile Phone
- Digital recording device (e.g. digital camera, audio recorder, MP3 player, etc.)
- Any other portable electronic device e.g. SatNav, etc.
- Memory sticks, cards, etc. (USB devices, SD cards, etc.)

2.2 Remote Working and Remote Access

Many organisations have business requirements to allow staff to work flexibly, using a variety of PEDs in a variety of locations. Remote working enables staff to work in any appropriate environment and may include remote access to IT systems. Examples of remote working include:

- Home working;
- Working when genuinely “on the move” (e.g. on a train or at the airport);
- Working at rest, including in hotels and coffee shops;
- Working in the office but using remote access technologies;
- Working from the premises of customers, delivery partners, contractors, or any other organisations.

Remote access allows users to access IT systems and resources from remote locations and can be considered to form a sub-set of remote working.

Remote working is anything other than the use of a fixed PC on a desk in the traditional office environment. This includes using PEDs in any environment (including the traditional office) and remote access to IT systems.

3. GUIDANCE FOR STAFF

"When using mobile computing and communicating facilities e.g. notebooks, palmtops, laptops, smart cards, and mobile phones, special care should be taken to ensure that business information is not compromised." ISO17799

3.1 Theft or loss of a PED

A PED used in a remote working environment is inherently vulnerable to loss or theft.

As PEDs can be lost or stolen, it is essential to implement security controls, such as encryption, to prevent any potential access to information stored within the PED. A thief or finder may deliberately attempt to discover information stored on a PED, pass it on to someone with greater capability or potentially use it to mount an attack on the organisation.

In order to minimise the potential for loss or theft, staff should ensure that PEDs are "**appropriately looked after at all times**".

- PEDs must **never** be left unattended in a car overnight
- PEDs must **never** be left unattended in open view in a car, at any time
- PEDs must **never** be left unattended in a public place e.g. on a train

Leaving a Council PED locked and out of sight in the boot of a car is acceptable providing:

- This is for a short period of time only e.g. for no more than 2 to 3 hours; and
- The PED has encryption software installed; and
- The PED is switched off, such that the encryption software is operational.

Leaving a Council PED unattended in a non-Council building is acceptable providing:

- The building/room is locked when leaving the PED unattended; and
- The PED is not left in open view; and
- The PED has encryption software installed; and
- The PED is switched off, such that the encryption software is operational.

Staff should exercise appropriate caution in public places against a forced attack where a PED may be taken while a member of staff is still logged in. However, staff should not put themselves or colleagues at risk to protect equipment.

A PED, even if encrypted, is a valuable asset and so should be afforded appropriate physical protection. Staff should "**treat a PED as though it were a large quantity of cash**".

Staff should be aware that leaving a PED in a locked hotel room may provide protection against opportunistic theft but is unlikely to prevent access by hotel staff.

Any theft or loss of a PED should be reported to the ICT Service Desk. Any theft or loss of a PED, which contains personal data or other sensitive business data, must also be reported to the Principal Information Security Officer.

3.2 Use of a PED overseas

The use or carriage overseas of a PED may increase existing and introduce new risks. The carriage of an encrypted PED overseas must be supported by a strong business case and authorised.

Approved Council PEDs or laptops may be taken to, and used within, countries within the European Economic Area providing a strong business case exists, encryption software has been installed and authorisation has been obtained from a Director or Head of Service.

PEDs must not be taken outwith the European Economic Area without first also obtaining authorisation from the Council's Data Protection Officer.

Users should note that nations might have specific regulations and laws relating to the carriage of cryptographic items across their borders and the use of cryptography within the country.

It is unlikely that staff can assert the same control over their physical surroundings when travelling or staying in hotels overseas. Staff should be aware that leaving a PED in a locked hotel room may provide protection against opportunistic theft but is unlikely to prevent access by hotel staff. Organised criminal groups, terrorists or investigative journalists may be able to operate more freely abroad.

When travelling overseas users should memorise any password and must not write it down anywhere. A search by customs or local police could compromise any written down or recorded password.

3.3 Procedural controls

The primary control to prevent loss of data on a PED is to "**avoid losing the PED**".

"**Data stored on the PED should be minimised to that necessary of the business requirement**". Users should not transfer significant quantities of data simply for convenience.

Data should be deleted from the PED when no longer required to perform the business function.

Users should not use PEDs containing, or providing access to, sensitive information where there is potential for loss of the PED while it is switched on. For example:

- Working in a busy public place such as a railway station;
- While transiting customs.

Back ups of any critical business information stored on a PED should be made regularly.

Users must not attempt to change the default security configuration of a PED e.g. disabling passwords, personal firewalls, anti-virus, etc.

3.4 Authentication (Usernames, Passwords, …)

Any passwords used should be sufficiently complex as detailed within Aberdeenshire Council Password Guidance - Simplifying our Approach.

If requested, a secure access token may need to be used as a secondary method of authentication. Dual-factor authentication improves security by relying on two means of authentication - something a user knows (password) and something a user has (a secure access token).

"**Staff must not store their passwords, or secure access tokens, along with the PED**". Loss of credentials along with the PED renders any encryption software ineffective.

3.5 Encryption software

The only effective method to secure sensitive data on a PED is to use Aberdeenshire Council approved encryption software.

"**Staff must not store their passwords, or secure access tokens, along with the PED**". Loss of credentials along with the PED renders any encryption software ineffective.

Staff must recognise that "**encryption software is only effective when a PED is switched off**". While the PED is in use, in sleep mode or in standby mode, no protection is applied.

3.6 Use of PEDs in Public places

Care should be taken when using PEDs in public places, meeting rooms, public transport, and other unprotected areas outside the organisation's premises.

Users of PEDs in public places should "**take care to avoid the risk of overlooking (shoulder-surfing) by unauthorised persons and to avoid PEDs being stolen**". See 3.1 for further information.

3.7 Use of privately-owned equipment (including Bring Your Own Device)

Privately-owned memory sticks, must not be used to store Aberdeenshire Council data: Guidance on use of flash drives.

Privately-owned equipment, must not be used to remotely access or store Aberdeenshire Council data except as permitted within BYOD section of Code of Practice: Acceptable Use of ICT Facilities i.e. where associated risks have been reviewed and mitigated via appropriate organisational and technical controls.

3.8 Disposal of PEDs

Nearly all PEDs contain memory which must be securely wiped before disposing of the PED.

PED disposal requirements are set out in Section 4.2 of Aberdeenshire Council's Code of Practice: Information Asset Classification.

Guidance on disposal of ICT equipment is detailed within AskFRED.

3.9 Use of Home Wi-Fi / Public Access Wi-Fi (Hotspots)

Users typically have a wireless router at home which is connected to the Internet - this provides a wireless network in the user's home. Vulnerabilities associated with using a home Wi-Fi network are similar to those when using a public Wi-Fi service.

Public Wi-Fi is commonly available in a number of locations including coffee shops, hotels and stations, providing access to the Internet either free or for a charge. A 'hotspot' is a location that offers Wi-Fi access to a customer via a wireless access point.

Having no security on your home network is not advised. If you have no security set on your home network, there is potential for Council information, and your own information, to be compromised. Similarly, WEP security is so weak that it can be compromised, with freely available tools, in a very short period of time. It is strongly recommended that you have your home network security set to either WPA or WPA2.

3.10 Asset Marking/Registration

All PEDs, with the exception of USB memory sticks and Council Mobile Phones, must be asset-marked and entered into the Aberdeenshire Council ICT Asset Register.

If a PED does not show a visible asset-mark, please log a call with the ICT Service Desk. To log a call with the ICT Service Desk please call 01224 664000, use the ICT Self Service Portal or send an email to ictservicedesk@aberdeenshire.gov.uk.

3.11 Personal use of Aberdeenshire Council owned PEDs

Limited personal use of Aberdeenshire Council owned PEDs can be made, providing any use is in accordance with Aberdeenshire Council Acceptable Use Policy and Code of Practice: Acceptable Use of ICT Facilities by Employees or in the case of Councillors the Code of Practice: Acceptable Use of ICT Facilities by Elected Members.

3.12 Use of Mobile Phones

The concept of a mobile phone being a device that only makes and receives telephone calls is not realistic. Current technology allows users to not only make telephone calls but also to browse the Internet, make Bluetooth connections, use camera functionality as well as store significantly large volumes of data.

Any use of camera functionality involving individuals should bear in mind Data Protection Act requirements.

Privately-owned mobile phones must not be used to remotely access Aberdeenshire Council data except as permitted within BYOD section of Code of Practice: Acceptable Use of ICT Facilities i.e. where associated risks have been reviewed and mitigated via appropriate organisational and technical controls.

3.13 Paper records

The following requirements apply to all sensitive paper records i.e. records containing: personal data or any other sensitive business information.

Prior to removing any sensitive paper records from Council premises, staff must ensure they have appropriate authority to do so. If necessary, they should check with their line-manager.

"**Any paper records to be removed, must be kept to the minimum required to meet the business requirement**". Staff should not move and carry around significant quantities of paper records simply for convenience. Taking electronic copies of documents saved to an encrypted Council laptop outwith Council offices is preferential to taking paper copies of documents outwith Council offices.

When removing paper records from the council's premises, for remote working purposes or for attending meetings, special care should be taken to ensure that information is not compromised.

Care should be taken when reading paper records in public places, meeting rooms, public transport, and other unprotected areas outside the organisation's premises. Staff reading paper records in public places should take care to avoid the risk of shoulder-surfing by unauthorised persons and to avoid paper records from being stolen. Shoulder-surfing is defined as looking over someone's shoulder to see what information they are handling.

Staff should be aware that leaving paper records in a locked hotel room may provide protection against opportunistic theft but is unlikely to prevent access by hotel staff. Where possible, paper records should be locked in the room's safe when the room is unoccupied.

Staff taking paper records home, or between Council premises, must ensure that data is appropriately looked after both in transit e.g. by securing them out of sight in the boot of the car or inside an anonymous document holder, and at home e.g. by storing them out of sight in a drawer or filing cabinet. Paper records not be readily accessible to family members or friends.

Where a member of staff is a full-time home worker the Council will consider providing a lockable filing cabinet for use at home.

When no longer required, any paper records removed from the council's premises must be returned to Aberdeenshire Council premises for filing or when required for secure disposal.

Prior to removing paper records from Council Offices, staff should ensure they have read and follow Council guidance on Secure Transportation of Paper Records.

3.14 Data Protection Awareness Training

Staff are not permitted to work remotely with Council personal data until such time as they have completed the Data Protection Awareness Course on ALDO. It should be noted that it is also a mandatory requirement to undertake Refresher Data Protection Awareness Training every three years.

A Scottish Local Authority has recently been found in contravention of the Act by permitting staff to work remotely without having first undertaken DPA training.

CODE OF PRACTICE

Revision Date	Previous Revision Date	Summary of Changes
15th August 2016	19th May 2015	Revised to remove complete prohibition of use of privately-owned equipment and add section 3.14 regarding DP training.
19th May 2015	December 2013	Revision and Distribution sections added.
December 2013	-	

DISTRIBUTION

The approved versions of these documents are distributed to:

Name	Title
Arcadia	Our Council/Information Governance/Information Security

Any copies of these documents out with the distribution list above is uncontrolled.