West Lindsey
DISTRICT COUNCIL
The Entrepreneurial Council

Information Governance

Remote Working Policy

JSCC Approved :
CP&R Approved:

Document Control

Organisation	West Lindsey District Council
Title	Remote Working Policy
Author	S M Anderson
Owner	ICT Manager
Subject	IT Policy
Review date	23/6/2015

Revision History

Revision Date	Revisor	Previous Version	Description of Revision
3/2/2011	Steve Anderson	Draft V0.2	Plain English guidelines applied.
21/3/2011	Steve Anderson	Draft V0.3	Para 6 – reference to Democratic Services Manager amended to Democratic Services Team Leader.
7/4/2011	Steve Anderson	Draft V0.4	Adopted by O&R Committee
2/7/2013	Steve Anderson	V1.0	Reviewed for PSN Compliance and minor amendments added.
23/6/2014	Steve Anderson	V2.0	Reviewed by Corporate Information Governance Group. Approved by CMT.

Contents

1 Policy Statement

West Lindsey District Council (the Council) gives some of its users the facilities and opportunities to work remotely through its Flexible Working Policy and Homeworking Policy. The Council will make sure that all users who work remotely are aware of the acceptable use of Personal Electronic Devices (PEDs) and remote working opportunities.

2 Key Messages

- All remote access must be approved and authorised by the user's manager. In the case of members' remote access, this is the Team Manager, People and Organisational Development.
- It is the user's responsibility to use PEDs in an acceptable way. This includes not installing software, taking due care and attention when moving PEDs and not emailing OFFICIAL information to a non-Council email address.
- Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location. Any security device provided by the Council must be fitted and used in accordance with the manufacturer's instructions.
- It is the user's responsibility to make sure that access to all OFFICIAL information is controlled – e.g. through password controls.
- All OFFICIAL data held on PEDs must be encrypted.
- Access to Council services from non-Council owned devices MUST be with an approved and authorised "Bring Your Own Device" (BYOD) solution and the information processed MUST NOT be classified OFFICIAL.

3 Purpose

The purpose of this document is to state the Remote Working Policy of the Council and should be read and applied with the Council's Flexible Working Policy and/or Homeworking Policy.

PEDs are provided to assist users to conduct official Council business efficiently and effectively. This equipment, and any information stored on PEDs, should be recognised as valuable organisational information assets and properly safeguarded.

4 Scope

This document applies to all councillors, committees, departments, partners, employees of the Council, contractual third parties and agents of the Council who use the Council Information and Communication Technology (ICT) facilities and equipment remotely. The document also applies to anyone who needs remote access to Council information systems or information.

5 Definition

This Policy should be adhered to at all times whenever any user makes use of PEDs. It applies to all use of Council ICT equipment and personal ICT equipment when working on official Council business away from Council premises (ie working remotely). Examples of remote working include:

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

This Policy also applies to all users’ use of Council ICT equipment and personal ICT equipment to access Council information systems or information whilst outside the United Kingdom.

PEDs are defined as any portable electronic device that has the ability to send, receive, record, process or store data. This includes, but is not restricted to:

- laptop computers;
- tablet computers;
- Personal Digital Assistant (PDA) or Smartphone;
- mobile phones;
- digital recording device (e.g. digital camera, audio recorder, MP3 player); and
- any other PED, such as a satellite navigation system or a hybrid device that combines functionality.

6 Risks

The Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business. The mobility, technology and information that make PEDs so useful to employees and organisations also make them valuable targets for thieves. Securing OFFICIAL data when users work remotely or beyond the Council network is important – particularly when protecting data in accordance with the requirements of the Data Protection Act 1998 (see the Legal Responsibilities Policy).

This policy aims to mitigate the following risks.

- The increased risk of equipment damage, loss or theft.
- Accidental or deliberate overlooking by unauthorised individuals.
- Unauthorised access to OFFICIAL information.
- Unauthorised introduction of malicious software and viruses.
- Potential sanctions against the council or individuals imposed by the Information Commissioner’s Office as a result of information loss or misuse.
- Potential legal action against the council or individuals as a result of information loss or misuse.
- Damage to the council’s reputation resulting from the loss or misuse of information.

Non-compliance with this Policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide services to our customers.

7 Applying the Policy

All remote access to Council information and services must be approved and authorised by the user's manager. In the case of members' remote access, this must be authorised by the Team Leader, People and Organisational Development.

All ICT equipment (including PEDs) supplied to users is the property of the Council and must be returned on request. Access for Council ICT staff shall be given to allow essential maintenance security work or removal on request.

All ICT equipment will be supplied and installed by Council ICT staff. Hardware and software **must only** be supplied by the Council.

Where users access Public Service Network (PSN) services and facilities or process OFFICIAL information, **under no circumstances** should non-Council owned equipment be used.

Where users access unclassified Council information remotely, this can only be from a council-owned and managed device or from a user-owned device which has been configured as part of an approved and authorised "Bring Your Own Device" (BYOD) solution. Contact the ICT department for more information.

7.1 User Responsibility

It is the user's responsibility to make sure that the following points are adhered to at all times.

- Remote access must be requested from the ICT Department. Users must say which applications they need to access.
- Users must take due care and attention of PEDs when moving between home and another business site.
- Users must not store usernames, passwords and authentication tokens with a PED.
- Users should not use a PED in any environment where it could be forcibly taken.
- Users should always fully shut down a PED when it is not in use. Data encryption is normally only effective when the PED is fully shut down.
- Users should make sure that no bystander can overlook any information displayed on a PED or any user input (especially passwords).
- Users must not install or update any software on to a Council-owned PED.
- Users must not install any screen savers on to a Council-owned PED.
- Users must not change the configuration of any Council-owned PED.
- Users must not install any hardware to or inside any Council-owned PED, unless authorised by the ICT department.

- Users will allow the installation and maintenance of Council-installed anti-virus updates immediately.

- Users will tell the ICT Helpdesk of any Council-owned PED message about configuration changes.

- Business critical data should be stored on a Council file server wherever possible and not held locally on the PED.

- All faults must be reported to the ICT Helpdesk.

- Users must not remove or deface any asset registration number.

- User requests for upgrades of hardware or software must be approved by the relevant manager using the Council's change request procedure. Equipment and software will then be purchased and installed by the ICT Department.

- The IT equipment can be used for personal use by staff as long as it is not used in relation to an external business. Only properly licensed software supplied and approved by the Council can be used (e.g. Word, Excel, Adobe, etc.) and other IT policies listed at Para 7.5 which stipulate the acceptable use of Council IT equipment MUST be followed (i.e. not accessing illegal or pornographic websites ect.).

- No unauthorised person including family members, friends etc. may use Council-supplied ICT equipment. The equipment is supplied for the sole use of the authorised user.

- The user must make sure that reasonable care is taken of any ICT equipment supplied. Where any fault in the equipment has been caused by the user, in breach of the above paragraphs, the Council may recover the costs of repair.

- The user should seek advice from the Council before taking any Council-supplied ICT equipment outside the United Kingdom. The equipment might not be covered by the Council's normal insurance against loss or theft and the equipment is liable to be confiscated by airport security staff.

- The Council may at any time, and without notice, carry out a software and/or hardware audit, and may ask for any equipment to be returned for further inspection. All users must fully co-operate with any request.

- Any user who chooses to work at home or remotely using their own ICT equipment as part of an approved and authorised BYOD solution must understand that they are not allowed to maintain any database, or carry out any processing of OFFICIAL information, about the Council, its employees, or customers.

- Any user using PSN services or facilities, or processing PSN OFFICIAL information, whilst working remotely, must only use Council-owned equipment which has approved technical security and advanced authentication mechanisms.

- **Under no circumstances** should OFFICIAL information be emailed to a private non-Council email address. For further information, please refer to the Email Policy.

7.2 Remote and Mobile Working Arrangements

Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.

Equipment should not be left where it would attract the interests of the opportunist thief. In the home it should be out of sight of the casual visitor. For home working it is recommended that the office area of the house should be kept separate from the rest of the house. A homeworking risk assessment should be carried out and approved by the user's manager. Equipment must be secured when not in use.

Where possible, the Council will provide suitable security devices with equipment for use in remote working locations. These devices can be an effective deterrent to an opportunistic thief. An example is the Kensington Lock which is used to secure a laptop computer to a fixed point such as a table leg. When a device has been supplied it **must** be fitted in accordance with the manufacturer's instructions. If you do not use security devices you increase the risk of Council information being lost or compromised and could be subject to disciplinary action. Any user concerned about security when working remotely should contact the ICT Team for advice.

Users must make sure that access/authentication tokens and personal identification numbers are kept in a separate location to the PED at all times. All removable media devices and paper documents must not be stored with the PED.

Paper documents are vulnerable to theft if left accessible to unauthorised people. These should be securely locked away in suitable facilities (e.g. secure filing cabinets) when not in use. Documents should be collected from printers as soon as they are produced and not left where they can be casually read. Waste paper containing OFFICIAL information must be shredded in accordance with the Information Management and Protection Policy.

7.3 Access Controls

It is essential that access to all OFFICIAL information is controlled. This can be done through physical controls, such as locking the home office or locking the computer's keyboard. Alternatively, or in addition, this can be done logically such as by password controls or User Login controls.

PEDs should be switched off, logged off, or the keyboard locked when left unattended, even if only for a few minutes.

All data on PEDs must, where possible, be encrypted. If this is not possible, then all OFFICIAL data held on the PED must be encrypted.

An encrypted Virtual Private Network (SSL or IPSec VPN) must be configured to allow remote users access to Council systems if connecting over public networks, such as the Internet. If connecting to PSN resources, this **must** be an IPSec-VPN.

The use of thin client over the VPN should be considered as a further means of security.

Dual-factor authentication must be used when accessing the Council network and information systems remotely.

Access to the Internet from Council-owned ICT equipment, should only be allowed via the Council’s proxy servers and not directly to the Internet.

7.4 Anti-Virus Protection

The ICT department will deploy an up-to-date anti-virus signature file to all users who work away from Council premises. Users who work remotely must make sure that their PEDs are connected to the corporate network at least once every two weeks to allow the anti-virus software to be updated.

7.5 User Awareness

All users must comply with appropriate codes and policies associated with the use of ICT equipment. This includes the following.

- Information Security Policy
- Information Management and Protection Policy
- Email Policy
- Internet Acceptable Use Policy
- Software Policy (TBA)
- PSN Acceptable Usage Policy and Personal Commitment Statement
- Computer, Telephone and Desk Use Policy
- Removable Media Policy
- IT Access Policy
- Information Security Incident Management Policy

It is the user’s responsibility to make sure that he/she is aware of and complies with these documents.

The user shall make sure that proper security measures are taken to stop unauthorised access to OFFICIAL information, either on the PED or in printed format. Users are bound by the same confidentiality and data protection requirements as the Council itself.

8 Policy Compliance

If any user is found to have breached this Policy, they may be subject to the Council’s disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this Policy or how it may apply to you, seek advice from the ICT department and/or your manager.

9 Review and Revision

This Policy will be reviewed as necessary, but no less often than every 24 months.

The Policy review will be carried out by the IT Manager supported by the Corporate Information Governance Group.

10 References

The following Council policy documents are directly relevant to this Policy, and are referenced within this document.

- Information Management and Protection Policy
- Information Security Policy
- Flexible Working Policy
- Homeworking Policy
- Email Policy
- Internet Acceptable Use Policy
- PSN Acceptable Usage Policy and Personal Commitment Statement
- Computer, Telephone and Desk Use Policy
- Bring Your Own Device Policy
- Removable Media Policy
- IT Access Policy
- Legal Responsibilities Policy
- Information Security Incident Management Policy

The following Council policy documents are indirectly relevant to this Policy.

- Human Resources Information Security Standards (TBA)
- IT Infrastructure Policy
- Communications and Operation Management Policy (TBA)