West Lindsey
DISTRICT COUNCIL
The Entrepreneurial Council

Information Governance

IT Access Policy

JSCC Approved :
CP&R Approved:

Document Control

Organisation	West Lindsey District Council
Title	IT Access Policy
Author	S M Anderson
Filename	
Owner	ICT Manager
Subject	IT Policy
Protective Marking	Not Protectively Marked
Review date	15/8/2014

Revision History

Revision Date	Revised By	Previous Version	Description of Revision
3/2/2011	Steve Anderson	Draft 0.1	Plain English guidelines applied.
7/4/2011	Steve Anderson	Draft 0.2	Adopted by O&R Committee
15/8/2013	Steve Anderson	V1.0	Document updated to remove references to the retired Imprivata OneSign system.
7/7/2015	Steve Anderson	V1.1	Document Approvals updated. Several minor typing errors corrected.

Contents

1. Policy Statement 4
2. Purpose 4
3. Scope 4
4. Definition 4
5. Risks 4
6. Applying the Policy – Passwords 5
6.1 Choosing Passwords 5
6.1.1 *Weak* and *strong* passwords 5
6.2 Protecting Passwords 5
6.4 System Administration Standards 6
7. Applying the Policy – Employee Access 6
7.1 User Access Management 6
7.2 User Registration 7
7.3 User Responsibilities 7
7.4 Network Access Control 7
7.5 User Authentication for External Connections 7
7.6 Supplier's Remote Access to the Council Network 8
7.7 Operating System Access Control 8
7.8 Application and Information Access 8
8. Policy Compliance 9
10. Review and Revision 9
11. References 9
12. Key Messages 10

1. Policy Statement

West Lindsey District Council (the Council) will establish specific requirements for protecting information and information systems against unauthorised access.

The Council will effectively communicate the need for information and information system access control.

2. Purpose

Information security is the protection of information against accidental or malicious disclosure (confidentiality), modification (integrity) or destruction (availability). Information is an important and valuable asset of the Council which must be managed with care. However, not all information has an equal value or requires the same level of protection.

Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorised use.

Formal procedures must control how access to information is given and how that access is changed.

This Policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

3. Scope

This Policy applies to all councillors, committees, departments, partners, employees of the Council (including system support staff with access to privileged administrative passwords), contractual third parties and agents of the Council with any form of access to the Council's information and information systems.

4. Definition

Access control rules and procedures are needed to regulate who can access Council information resources or systems and the associated access privileges. This Policy applies at all times and should be adhered to whenever accessing Council information in any format, and on any device.

5. Risks

Occasionally, business information may be disclosed or accessed prematurely, accidentally or unlawfully. Individuals or companies, without proper authorisation and clearance may intentionally or accidentally gain unauthorised access to business information which may adversely affect day to day business. This Policy is intended to mitigate that risk.

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 necessary services to our customers**.**

6. Applying the Policy – Passwords

6.1 Choosing Passwords

Passwords are the first line of defence for our ICT systems and together with the user ID and any 2-factor authentication device help to establish that people are who they claim to be.

A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.

This password policy has been written with regard to CESG's *Password Guidance: Simplifying Your Approach* which has been produced to help users cope with "password overload".

6.1.1 *Weak* and *strong* passwords

A weak password is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

A strong password is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

Everyone must use strong passwords with a minimum standard of:

- At least ten characters.
- Contain a mix of alpha and numeric, with at least one digit
- More complex than a single word (such passwords are easier for hackers to crack).

6.2 Protecting Passwords

It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to at all times:

- Never reveal your passwords to anyone.
- Never use the 'remember password' function.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different council systems (unless "single sign on" has been enabled across multiple systems).

- **Do not use the same password for systems inside and outside of work**.

6.3 Changing Passwords

All user-level passwords must be changed at a maximum of every 365 days, or whenever a system prompts you to change it. Default passwords must also be changed immediately. If you become aware, or suspect, that your password has become known to someone else, you must change it immediately and report your concern to the ICT helpdesk.

Users must not reuse the same password within 5 password changes.

6.4 System Administration Standards

The password administration process for individual Council systems is well-documented and available to designated individuals.

All Council Information and Communication Technology (ICT) systems will be configured to enforce the following.

- Authentication of individual users, not groups of users and no generic accounts.
- Protection with regards to the retrieval of passwords and security details.
- System access monitoring and logging at a user level.
- Role management so that functions can be performed without sharing passwords.
- Password administration processes which are properly controlled, secure and auditable.

7. Applying the Policy – Employee Access

7.1 User Access Management

Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to allow authorised user access and to prevent unauthorised access. Procedures must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer need access. The procedures must be properly authorised. Each user must be allocated access rights and permissions to computer systems and data that:

- are commensurate with the tasks they are expected to do;
- have a unique login that is not shared with or disclosed to any other user; and
- have an associated unique password that is requested at each new login.

User access rights must be reviewed at regular intervals to make sure that the proper rights are still allocated. System administration accounts must only be given to users that need to perform system administration tasks.

7.2 User Registration

A request for access to the Council's computer systems must first be created by People and Organisational Development (POD), and approved and authorised by the user's manager (in the case of members this will be the Team Manager, People and Organisational Development). The request must include confirmation that the user has read and signed the IT Access Policy. Only when both manager and POD approvals have been completed can the ICT Team create the user account.

When an employee or member leaves the Council, their access to computer systems and data must be suspended at the close of business on their last working day. It is the responsibility of the leaver's manager to request the suspension of the access rights and the responsibility of the IT Department to suspend the access and action any specific instructions regarding the leaver's data.

7.3 User Responsibilities

It is the user's responsibility to prevent their user ID and password being used to gain unauthorised access to Council systems by:

- following the password policy statements outlined above in Section 6;
- making sure that any computer they are using that is left unattended is locked or logged out;
- leaving nothing on display that may contain access information such as login names and passwords, including the USB memory stick containing the encryption key; and
- informing the ICT Team of any changes to their role and access requirements, via a request approved by their line manager.

7.4 Network Access Control

The use of modems on non-Council owned computers connected to the Council's network can seriously compromise the security of the network. The normal operation of the network must not be interfered with. Specific approval must be obtained from ICT Team before connecting any equipment to the Council's network. This includes USB Memory Sticks, external hard drives, external zip drives.

7.5 User Authentication for External Connections

Where remote access to the Council's network is needed, a Remote Access Application must be made by the user's service manager. Remote access to the network can be provided from a Council-supplied tablet computer. For

further information please refer to the Remote Working Policy or contact the ICT Team.

7.6 Supplier's Remote Access to the Council Network

Partner agencies or 3rd party suppliers must not be given details of how to access the Council's network without permission from the ICT Team. Any changes to supplier's connections must be immediately sent to the ICT Team so that access can be updated or ceased. All permissions and access methods must be controlled by ICT Team.

Partners or 3rd party suppliers must contact the ICT Team before connecting to the Council network and a log of activity must be maintained. Remote access software must be disabled when not in use.

7.7 Operating System Access Control

Access to operating systems is controlled by a secure login process. The access control defined in the user access management section (section 7.1) and the password section (section 6) above must be applied. The login procedure must also be protected by:

- not displaying any previous login information e.g. username;
- limiting the number of unsuccessful attempts and locking the account if exceeded;
- hiding the password characters by symbols; and
- displaying a general warning notice that only authorised users are allowed.

All access to operating systems is via a unique login id that will be audited and can be traced back to each individual user. The login id must not give any indication of the level of access that it provides to the system (e.g. administration rights).

System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day to day activities.

7.8 Application and Information Access

Access within software applications must be restricted using the security features built into the individual product. The Corporate Systems Manager or departmental administrator of the software application is responsible for granting access to the information within the system. The access must:

- be compliant with the user access management section (section 7.1) and the password section (section 6) above;
- be separated into clearly defined roles;
- give the appropriate level of access required for the role of the user;

- be unable to be overridden (with the administration settings removed or hidden from the user);
- be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access; and
- be logged and auditable.

8. Policy Compliance

If an employee is found to have breached this policy, they may be subject to the Council's disciplinary procedure. If a member is found to have breached the policy then this may be dealt with in accordance with the Members' Code of Conduct. 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 People and Organisational Development department.

10. Review and Revision

This Policy will be reviewed as it is deemed appropriate, but no less often than every 12 months.

The Policy review will be undertaken by ICT Manager supported by the Corporate Information Governance Group.

11. References

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

- Remote Working Policy.

The following Council policy documents are indirectly relevant to this policy:

- Email Policy.
- Internet Acceptable Usage Policy.
- Software Policy.
- PSN Acceptable Usage Policy and Personal Commitment Statement.
- Legal Responsibilities Policy.
- Computer, Telephone and Desk Use Policy.
- Removable Media Policy.
- Information Protection Policy.
- Human Resources Information Security Standards.
- Information Security Incident Management Policy.
- IT Infrastructure Policy.
- Communications and Operation Management Policy.

12. Key Messages

- All users must use a unique username and complex password to access the network.
- The USB memory stick containing the encryption key must be protected at all times and not left on the desks.
- User access rights must be reviewed at regular intervals.
- It is the user's responsibility to prevent their user ID and password being used to gain unauthorised access to council systems.
- Partner agencies or 3rd party suppliers must not be given details of how to access the council's network without permission from ICT Team.
- Partners or 3rd party suppliers must contact the ICT Team before connecting to the council network.