The Linden Centre

Networks Policy

Signed by:		
	Headteacher	Date:
	Chair of Management Committee	Date

Last Updated	04th January 2021
Review Due:	04th January 2022

S8 Computer Networks Use (v6.0)

Computer networks include:

- virtual private networks (VPN)
- direct access
- local area networks (LAN)
- wide area networks (WAN)
- wireless networks
- network storage

Virtual private networks

A VPN is a secure network that will allow staff to access the council network if a direct link to the council network is not available.

Direct Access

For Windows 8.1 machines the Council has implemented Direct Access for remote access. Direct Access is an accredited solution for allowing secure remote access to Council IT resources without the need to use VPN.

Local area network, wide area networks and wireless networks

Access to the Council's networks is given to staff that have a need to use it.

This service can be revoked at any time by ICT if there is unacceptable use of the networks.

The networks are the infrastructure of the Councils systems and as such are used via equipment that staff will have access to. Information travelling the network may be monitored in line with the Lawful Business Practices Regulations 2000.

Wireless network access to the Council networks is available to a wireless enabled device. Third party access is also available on the Council's Guest Network. Guest access can be acquired by using Access Codes that are available from the intranet.

Network storage

As mentioned elsewhere in this policy network drives are the locations of information stored on the Council network. The C drive, the drive physically inside a PC or laptop is not a network drive and will not be backed up.

The "home drive" (commonly known as the H: drive) on the Council network, is a networked storage area specifically for an individual to store information. The H drive is normally backed up however; **confidential information must not be stored here** as ICT reserve the right to not backup these drive(s). This also applies to the use of One Drive.

No personal information of any kind must be stored on any computer drives, networked or otherwise, including video, pictures or music that are non-work related.

Shared drives are networked drives that must be used to store, manage and share information with colleagues. Restricted areas can be set up on shared drives or sharepoint sites to keep information confidential to teams. Contact ICT if this facility is required.

Storage of any information and files that can be considered obscene, pornographic or fall within any of the other unacceptable uses specified in section 6 is not allowed and will result in disciplinary action and where appropriate, police action.

Any information stored on network drives may be monitored and opened in line with the Lawful Business Practices Regulations 2000.

Service Delivery Managers take responsibility within their areas for where and how information is stored (in any format).

The security of the council's information is of paramount importance, to protect the ability of the council to provide services, and in the case of personal data to protect the privacy of the individual. When saving confidential information to network drives consideration must be given to who has access to that area and whether or not it is appropriate to store the information there.

File retention and destruction rules exist for all information within the council that govern how long information must be held. Access the Corporate Information Retention Schedule (CIRS) via the Information Governance intranet page or contact Information Governance for more information on good records management including retention and destruction.

Backups

ICT will backup corporate systems in line with their backup policies and procedures. Data will be backed up to an offsite data centre weekly, with updated files backed up locally on a nightly basis.

Users should be aware that all confidential and critical information should be stored on the corporate networks.

The "local drives" on PC's (commonly referred to as the C: drive) are not backed up by ICT.

ICT also reserves the right to reduce the backup frequency, or cancel backups of the "home drive" (commonly known as the H: drive). If this becomes the case all affected staff will be informed and asked to move critical files to other locations on the network.

OneDrive is not backed up by Microsoft, however if any file is deleted, it can be recovered via the recycle bin in OneDrive. Data stays in the recycle bin for up to 6 months and can be recovered as long as the item is not permanently deleted from the recycle bin.

Other ICT Responsibilities

- ICT will undertake the following tasks in respect to Council networks:
- Ensure that server configuration/security complies with relevant server configuration/security standards
- Ensure that patches are applied to all relevant servers on a timely basis relevant to their release
- Ensure that appropriate change control processes are followed in respect to server changes
- Provide router/switch management services
- Use diagnostic tools to ensure networks are running securely at optimum levels
- Ensure up to date and fit for purpose anti-virus solutions are deployed on Council servers and end user work devices.