The Linden Centre

The Linden Centre

Equipment Policy

Signed by:		
	Headteacher	Date:
	Chair of Management Committee	Date

Last Updated	12/12/2022
Review Due:	12/12/2025

S1 Acceptable Use of Equipment & Media (v6.0)

This section covers the acceptable use specific to work equipment that staff may use. It also covers staff using their own devices to access Council services via the corporate cloud.

It is important that all staff are aware of the types of equipment that the Council uses and what is acceptable and unacceptable.

Any computer equipment, be it storage, computer, application or mobile phone must be purchased through ICT and be authorised to connect to the Council's networks and systems. Computing resources not owned by the Council must not be connected to the Council's network unless via O365.

If you lose or have your ICT equipment stolen this is considered a security breach. The incident should be reported immediately to the ICT Service Desk/Information Governance and the Information Security Breach Procedure followed.

Personal Computer (desktop)/Laptop/Tablet Use

For personal computer/laptop tablet use staff must abide by the tables below.

Acceptable

Computers are provided to staff in order for them to carry out their role within the Council

When left unattended staff should lock their computers so that they cannot be accessed by others. This is activated by pressing the ctrl-alt-del buttons simultaneously and selecting "Lock Computer" or holding down the windows key and pressing 'L'

Any media being used to transfer data from a laptop to another piece of Council equipment must be procured via ICT

Accessories and laptop or tablet PC equipment must be purchased through ICT.

Unacceptable

Software and files must not be downloaded from the Internet without ICT approval

Confidential information must not be accessed in a public place where unauthorised persons may view information displayed on the screen

Laptop and tablets must not be left unattended in an insecure area. The boot of a car is an acceptable storage place for mobile workers who have to leave equipment in a vehicle unattended for short periods of time. However any Council equipment including laptops and tablets must not be left in a vehicle overnight or over a weekend

Files of a personal nature, such as images for example, must not be stored on the local drive (more commonly known as the C drive) or on any network drives such as your homes (h) drive or shared network storage area

Staff must not allow access to their computer/laptop (when they are logged on) to any other staff members. The staff member logged in to the pc/laptop is responsible for any actions completed with their user id/password

Staff owned devices

Staff can use their own laptop/pc to connect to the corporate cloud services that the Council provides. To use a non-windows based client (Apple-IOS, Android, etc) an approved request for this type of access needs to be sent to ICT.

In general the Council does not allow staff to use IPADS to access the Council's network services directly as these types of devices are not deemed 'secure' and therefore are not approved devices.

However in some circumstances the Council will allow staff to use personal IPADS to access some Council services if the member of staff completes a 'Personal Devices Condition of Use Form', has this approved and forwards this to the ICT Service Desk.

Anti Virus

ICT Responsibility

- It is the responsibility of ICT to ensure appropriate anti-virus software is installed on all work desktop computers, laptops and tablets that connect to the council's network.
- ICT are also responsible for sending updates to the anti-virus software.

Officer Responsibility

Officers must:

- Not disable the anti-virus software, or software of a similar function or any automatic update facilities on council PC
- Inform ICT if their anti-virus software appears to not be working or updating correctly
- Virus check any media being used to transfer data from a laptop to another piece of council equipment
- Not knowingly distribute or otherwise be involved in virus, trojans, malware

Multi-Functional Devices

Officer Responsibility

Officers must:

- Ensure work documents are not left unattended on the MFD
- Not leave a jam in the MFD in case when the jam is resolved their document prints unattended
- When using the scan to me option officers must ensure they check the receiving email address on the MFD is correct