The Linden Centre

The Linden Centre

Internet Policy

Signed by:		
	Headteacher	Date:
	Chair of Management Committee	Date

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

S3 Use of Internet (v6.0)

The use of the internet is a valuable business tool, but staff must be aware that the internet should be used responsibly.

Key Messages

- All internet use via the Council's equipment/systems/mobiles will be monitored.
- Officers can only use the Council's internet facility for personal use in non-work time and in compliance with the usage set out in this document.
- Misuse of the internet can lead to disciplinary or criminal proceedings

For internet use staff must abide by the tables below

Acceptable

Only access the internet for personal reasons in non-works time with access complying with the requirements of this policy.

Ensure personal use of the internet complies with the requirements of this document.

Consult with ICT before downloading software from the internet

Report any information found on the internet that may be inaccurate or defamatory to the Council or its officers to their line manager

Report accidental unauthorised internet access, i.e. when they received an 'Access Denied' system message, to their line manager

Unacceptable

Breach the confidentiality of individuals or the Council

Run a business of profit making activity including auction site

Access websites for personal use during work hours

View websites that are not allowed by the Council on Council equipment/using Council infrastrucuture, including but not limited to:

Video and audio files
Photo searches
Sexually explicit/pornographic
Intolerance/hate
Criminal action
Tasteless/Offensive
Chat groups/rooms
Violence/weapons
Illegal drugs
Hacking
Spyware
Proxies and translators
Sex education
Fraud
Phishing (fraudulently obtaining sensitive information such as passwords, bank details, etc, by pretending to be a trustworthy source)

Download software or utilities to corporate equipment without authorisation

Publish or make available confidential or personal data via websites, newsgroups, forums, social networking/media sites or any similar facility. For more guidance on the appropriate use of social medial sites please see the Social Media Policy

Represent their own opinions as those of the Council on any websites

Knowingly distribute or otherwise be involved in virus, Trojans or other malware use

Post Council information on personal social media sites

Internet Monitoring

The Council reserves the right to monitor the use of the Internet and web in line with the Lawful Business Practice Regulations (2000) for the purposes of:

- gaining routine access to business communications
- monitoring standards of service and training
- prevention or detection of crime
- detecting unauthorised use of the internet.

Staff must be aware that the Council cannot guarantee privacy of staff private information if they use webmail or Internet banking and supply passwords and other security details to gain access to these facilities.

The Council reserves the right to block access to any website deemed inappropriate and to report access of inappropriate material to Human Resources/Audit & Governance in the event that this type of activity is logged. Misuse of the internet can lead to disciplinary action being taken.