The Linden Centre

Work Mobile Phones Policy

Signed by:		
	Headteacher	Date:
	Chair of Management Committee	Date

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

Telford & Wrekin COUNCIL

S4 Mobile Phone Use (v6.0)

NOTE: Work devices must not to be used for personal purposes

The term mobile phone includes but not limited to:

Mobile Phones	Smart Phones	Other 'sound picture voice' (SPV) devices

These devices, as with all Council equipment, are provided for work use only.

For mobile devices staff must abide by the tables below

Acceptable

Always use PIN security provided on phones
Conduct all verbal and text (where text is appropriate) conversations in a professional manner and within the Councils acceptable standards of behaviour
Be aware of your surroundings, e.g. do not discuss confidential matters where they could be overheard, i.e. on a crowded train
Ensure that all files stored on mobile devices are moved to the corporate network so that they are back up. Regular synchronisation with your corporate PC will enable this to be performed. Files should then be removed from the mobile device.
Close down the mobile device when not using it to prevent unauthorised access
Follow any separate Acceptable Use Agreement (AUA) for Council provided mobile phones

Unacceptable

Never call or access inappropriate numbers, e.g. chat lines, premium rate numbers
Never use cameras on devices to take inappropriate, pornographic, obscene, discriminatory or otherwise offensive images
Never download unauthorised software including ring tones
Never allow anyone else to use the device including family, friends and children

Never leave the device unattended/unsecured or in a parked car

Do not use mobile devices whilst driving (unless using hands free facilities)

Monitoring of mobile devices

Mobile devices may be recalled at any time by ICT or Audit & Governance to check compliance with this policy. All monitoring will be done in line with the Lawful Business Practice Regulations 2000.

Security of mobile devices

It is the user's responsibility to ensure that the physical device and any information stored on it is as secure as possible.

All Council information must be regularly transferred to the corporate networks to ensure it is backed up. Mobile devices are not automatically backed up.

If a device is lost or stolen it must be reported to the police immediately (if stolen) and a crime reference number obtained. It should then be reported to ICT/Information Governance as per the Information Security Breach Procedure.

Never attempt to factory reset your work mobile phone without ICT support