Leicester City Council

Information & Support
Policies and Guidance

Use of Personal Device(s) Policy

July 2019

Document Version: V1.
Review Date: June 2020
Owner: City Information Officer

1. Introduction and Purpose

1.1 Leicester City Council recognises the benefits that can be achieved by allowing staff to use their own mobile computing devices when working, whether that is in an office, at home, or while travelling. Mobile computing devices include laptops, smart phones, tablets or any mobile networked computing device with the capability to access the Council's networked resources or services.

1.2 'Personal devices', typically referred to as Bring Your Own Device' "BYOD", refers to computing devices that are not supplied or managed by the Council.

1.3 This policy aims to safeguard the confidentiality, integrity and availability of Council services and data held on personal devices.

1.4 The use of personal devices for business purposes will be subject to monitoring and periodic review.

1.5 No employee is required to use their personal mobile devices for business purposes. It is a matter entirely for each person's discretion. Staff are encouraged to consider carefully how and when they use their devices and disable work related functions when on leave to ensure they maintain an effective balance between work and personal life.

1.6 This policy supplements, and should be read in conjunction with, the council's other information security policies and procedures in force, located here Information Security Policies and the Information Governance and Risk Policy

1.7 The Council Skype for Business Application will be installed as standard for all users so that staff only need to provide their Council landline (0116 454 xxxx) business number for any business use over using their personal mobile number

2. Scope

2.1 This policy applies to all employees electing to use their personal device to receive the services available on equivalent LCC corporate devices including, for example, business calls, emails, calendars, collaboration tools, data and applications.

2.2 This policy excludes elected councillors who already receive a telecommunications and support allowance under the approved members allowances scheme.

3. General Responsibilities

3.1 The safeguarding of personal devices used for business purposes remains the employee's responsibility. The Council takes no responsibility, and will not recompense any employee, for the loss of, or damage to, a personal device used for business purposes. Thus, the full cost of repairing or replacing any personal device shall be borne by the employee.

3.2 As a personal device is to be used for business purposes primarily during working hours, using the device for personal reasons should not interfere with the employee's performance of their duties.

3.3 Wherever possible, users are encouraged to connect their personal device to WIFI for data usage instead of using their data allowance. The council, in return, will permit users to connect their personal devices to an appropriate network.

4. Security Requirements

4.1 Employees must:

- use the device security features, such as a PIN, biometrics, password or passphrase, to protect the device when not in use.
- set screen locks to ensure that their personal device locks automatically when not in use.
- keep the device software/firmware up to date.

4.2 If an employee's device supports the following services they are encouraged to be activated and used/installed and configured:

- encryption services.
- anti-virus protection.
- tracking and/or wiping services, such as Apple's 'Find My iPhone app', Android's 'Where's My Droid' or Windows 'Find My Phone'.

4.3 Employees must not:

- use any personal device where the manufacturer's security mechanisms have been circumvented, such as 'Jailbreak', to access Council systems or data.
- allow other persons to access and use council data, software and systems on their personal device
- use their personal device to deliberately compromise, or attempt to compromise, the confidentiality, integrity or availability of council or non-council systems or data.
- use their personal device to access unapproved Cloud Hosted storage (e.g. Dropbox) to store council data.

4.4 The personal device must be enrolled in the LCC Mobile Device Management (MDM) service. If an employee's mobile device is lost or stolen, the MDM system will be used to remotely wipe the device of LCC content.

4.5 When an employee leaves the Council, it is the responsibility of the line manager to follow the leavers process to advise Information Services who will thereafter ensure that LCC content is remotely removed from the device.

5. Council Contribution Scheme

5.1 Where an employee is eligible for a council owned mobile device under the **Corporate Mobile Communications and Acceptable Use Policy** they may choose instead to use their personal device for business purposes, e.g. for voice calls, SMS and data. In

these circumstances the council will contribute towards the employee's monthly personal payment plan in respect of business calls and data used. The contribution as at 1st July**2019 is £15.00** per month.

5.2 The contribution will be paid with the employee's salary each month and the payment will be treated as normal income for tax purposes .

5.3 The contribution is not intended to cover any calls to premium rate numbers, overseas calls and for use whilst abroad and these are not encouraged for business use. However, where there is a **business need** only for such calls, authorised by the relevant Head of Service, the cost may be claimed as an expense. Evidence of calls must be provided to support the claim.

5.4 An employee opting to use their personal device for business purposes in lieu of a council owned device will be required to sign an agreement.

5.5 The employee must self-select, and maintain responsibility for, a monthly payment plan with their provider that best suits their expected combined personal and business usage each year.

5.6 Payment of the full costs of the plan to the provider remains the responsibility of the employee. Employees who exceed their payment plan will be responsible for the resultant payment themselves and the council will not recompense any such charges.

5.7 Contribution rates will be reviewed at least annually and any changes in tariffs in the market prevailing at the time will be considered. All users will be notified if there is any change to the contribution rate in advance and the date from which they will be applied.

6. Breach of this Policy

6.1 Non-compliance with the responsibilities set out in this policy will be treated as misconduct and disciplinary action may be taken up to and including dismissal. Civil or criminal prosecution could also result from breaches of the Data Protection Act 2018 and related legislation involving council data. Disciplinary action may be taken whether the breach is committed during or outside working hours and whether or not use of the device takes place at the employee's normal place of work. Employees are required to co-operate with any investigation into suspected breach which may involve providing access to the device and any relevant passwords and log in details.

6.2 Breach of this policy could result in an employee's eligibility being withdrawn.

7. Support for Use of Personal Devices

7.1 IT Services will assist with setting up and connecting a personal device to council systems if the device supports this. Employees are responsible for learning how to use their devices effectively.

7.2 The Council takes no responsibility for the ongoing support or maintenance of an employee's personal device or any user downloaded apps.

7.3 Any user downloaded applications are found to have security vulnerabilities, they must be removed from the personal device upon the instruction of IT Services. If they are not removed access to Council services or data will be removed.

7.4 IT Services will only assist in changing passwords of council systems and applications accessed by the personal device. Passwords for personal (non-council) systems and services must be changed by the employee.

7.5 If a personal device that has been used to access council services is lost or stolen, this must be reported to the Information Governance team immediately.

7.6 If an employee suspects that their personal device has been compromised, they must report this to the IT Service Desk immediately on 0116 454 1066.

8. Monitoring

8.1 The council will not monitor the content of an employee's personal device. However, the council reserves the right to monitor and log data traffic transferred between a personal device and council systems.

8.2 In exceptional circumstances, for instance:

- where the council requires access to comply with its legal obligations (e.g. under Data Protection or Freedom of Information legislation); or
- where obliged to do so by a court of law or other law enforcement authority; or
- in accordance with paragraph 6.1 of this policy

the council will require access to the personal device used for business purposes. Under these circumstances all reasonable efforts will be made to ensure that the council does not access private information.