Mobile Device Policy

1 Version History details and author

1.0	05/06/2020	Re-write of mobile telephony following centralisation and update to ICT administration	Sarah Wallis
1.1	2/07/2020	Review by Internal Audit	Spenser Geeson & Phil Spencer
1.2	30/07/2020	Changes by ICT Services	Mark Whelan
1.3	26/08/2020	Changes by ICT Services	Joe Lynch
1.4	06/09/2020	Small revisions / clarifications	Mark Whelan / Internal Audit
1.5	09/09/2020	Clarification included on use of personal mobile calls following IGG discussion 08/09	Mark Whelan
2.0	05/10/2021	Reviewed by Information Governance Group.	Jo White
3.0	04/10/2022	Reviewed by Information Governance Group. Reference to switching geo location off added. Policy links updated.	Jo White
4.0	14/11/2023	Reviewed by Information Governance Group. Reference to switching geo location off added. Policy links updated.	Jo White
5.0	12/11/2024	Reviewed by Information Governance Group. Updated to cover personal mobile devices.	Jo Williams

This document has been prepared using the following ISO27001:2022 standard controls as reference:

ISO Control A 5.10 - Acceptable use of information and other associated assets.
ISO Control A 5.12 – Classification of Information
ISO Control A 5.14 - Information transfer
ISO Control A 5.15 – Access control
ISO Control A 6.7 – Remote working
ISO Control A 6.8 - Information security event reporting
ISO Control A.7.8 - Equipment siting and protection
ISO Control A.7.9 - Security of assets off-premises
ISO Control A.7.10 – Storage media
ISO Control A.7.13 - Equipment maintenance
ISO Control A.7.14 - Secure disposal or re-use of equipment
ISO Control A 8.1 – User endpoint devices

2 Introduction

Derbyshire County Council recognises the importance of technologies which enable users to carry out their day to day business effectively. Good communication is vital to the running of the Council and its services. Communication devices such as mobile phones are widely used by users and are increasingly relied on, not only to provide voice and text messaging but also e-mail and other internet enabled resources and services.

As with any other IT related equipment and resources, the Council needs to ensure that the use of corporate mobile devices is organised and controlled in a manner which will be beneficial to the safety, integrity and reputation of the Council. The Council also allows limited use of personal mobile devices for accessing Council resources such as email, Teams and approved systems.

To ensure a consistent approach is adopted across all departments, procedures exist for the provision, ordering, reporting lost or stolen and disposal of corporate mobile devices. This policy covers all mobile devices and related equipment, whether these are issued to an individual or as part of a departmental pool.
The policy also relates to personal mobile devices that are being used for business purposes.

Additionally, there are user guides available via Halo to assist with many of the associated functions of a smartphone.

Access to Halo: Self-Service Portal (derbyshire.gov.uk).

3 Purpose

The purpose of this policy is to ensure users are aware of the controls and methods the Council has put in place to manage and secure mobile devices. Users are expected to comply with the policy to ensure that devices and data are protected, and the Council's ICT computer network and devices are appropriately secured from unauthorised access and compromise.

4 Scope

This policy applies to the use and configuration of all mobile devices that have been provided by the council (corporate) and personal devices which are used for accessing Council systems. The policy covers all employees, agency staff, elected members, contractors, volunteers, apprenticeships, student/work experience placements and partner agencies who have access to these devices, described as "users" within this document.

All corporate Mobile Devices include Smartphones, Non-Smartphones, Dongles, tablets with SIMs, SIMs and MiFi devices are also covered by the policy.

5 Policy Statement

All mobile devices issued by the Council, must only be used for Council business and used as a communications and "resource" tool. This means telephone calls, text messaging, access to Council systems and using the Internet in line with the Council's Internet and E-mail Policy (see Appendix 1).

Mobile devices supplied by Derbyshire County Council, are not to be loaned or given out to anyone else, unless in exceptional circumstances where appropriate management authorisation has been granted and a record is kept of any temporary transfer of use.

6 General

Mobile devices supplied by the Council are for work related use only, unless it is an emergency. If a user is called out at short notice or is required to work later than planned and needs to advise their family a short call is treated as business purposes.

Whilst it is accepted that a member of staff may use a personal device to make calls relating to the Council's business, they should do so in line with the Council's information security and HR policies.

All corporate smartphones are registered on the Council's Mobile Device Management (MDM) system before being issued to staff. Staff are then required to enrol their phone onto the MDM. This ensures that such devices can be managed for security updates and remotely wiped and disabled if they are lost or stolen. Where a member of staff needs to use their own personal mobile telephone including, to make calls or texts, they should do so.

Where there is a service need staff should be provided with a corporate mobile device. By requesting / taking ownership of a corporate mobile device employees/managers are confirming their acceptance of the Council's procedures relating to its use. It is important that records are maintained on where mobile devices are allocated and these are updated as staff move positions or leave.

Where mobile devices are not assigned to individual users and are used as pool devices, a localised record of users should be maintained by the assigned department lead and should include the users' details, purpose and dates of assignment. By using these devices individuals are confirming their acceptance of the Council's procedures.

When using a mobile device, users must exercise caution and consider their immediate environment when making confidential calls. Further information on Data Security is available on the Council's website (see Appendix 1).

Users should ensure that they take their allocated Corporate mobile device with them when they leave their base unless the device is kept (locked away) securely when not required.

Corporate mobile devices should always be switched on during working hours, or when on-call, except where it would be inappropriate for the device to ring e.g. in meetings, whilst driving etc.

It is the user's responsibility to keep their allocated corporate mobile device and any associated equipment operational and safe. Bumper cases and screen protectors are provided and should be used.

Users should not leave a mobile device unattended where it can easily be seen and/or stolen.

SIM cards should not be removed from a device unless instructed to by a member of ICT Services. Any request to transfer a corporate mobile device or SIM needs to be undertaken in consultation with ICT Services using Service Desk Online. Links to the appropriate forms can be found in Appendix 1.

The automatic keypad/screen lock should be enabled at all times on mobile devices. Unless it is not possible for operational reasons, mobile phones should be protected

by a PIN access code. Staff should not share PIN codes or other password details with anyone else. It is recognised that this cannot be enforced on personal devices.

Multimedia memory cards should not be inserted in corporate mobile devices.

Where the device has the capability of dual SIM technology, the user must not fit a second SIM card in the device.

Mobile devices should not be used when driving or controlling any vehicle.
Calls should only be taken when it is safe to do so. A link to the Safe Use of Mobile Phones guidance can be found in Appendix 1.

Near Field Communication should not be activated or used, except in approved circumstances.

If Bluetooth is used to connect a smartphone to a car for hands free communication, the user should be mindful that the car can save contacts, recent calls, text messages and GPS data to the car's data storage facility and this is subject to both the Council's data management and Safe Use of Mobile Phones policies. Users are responsible for ensuring that all data is removed from the car's data storage facility. In the event the user is not able to delete the data they should contact the hire company to make arrangements to have their data deleted.

There must be no trace of sensitive or personal data including username and/or passwords left on any type of mobile device which could be used to provide unauthorised access to Council systems and data. Unless not technically possible, all Council mobile devices including phones will have encryption applied. It is recognised that this cannot be enforced on personal devices.

7 Making Calls

All corporate mobile devices have an automatic bar on International and Premium rate calls, texts and SMS subscription services. The default bar can be lifted in specific circumstances by ICT Services, where justification is provided by the user and Senior Manager approval is obtained. Where International calls need to be made for official Council business users should always endeavour to use a landline as international mobile calls are charged at premium rates from mobile devices.

Calls to 118 Directory Enquiries can be expensive and users should avoid their use. In cases of emergency where directory services are required users should try and use 0800 118 3733. Users should decline any offers to put them through to the requested number and then end the call (due to additional call charges). They should then call the requested number directly.

8 Text Messages, Use of Camera & Video including Geolocation

Mobile devices should not be used in any manner which would or could cause harassment or distress to any member of public or service users – including the distribution of inappropriate text messages/images or the capturing of images/video.

Where text messages, images or video are captured the user should ensure that such data is being processed and manged in accordance with the Council's corporate data protection policy and the Data Protection Act 2018.

Sensitive and personal information must never be sent by text message as it is not a secure method.

While carrying out day-to-day tasks, if a user must use the camera or video function on their allocated mobile device, they should always be aware of their surroundings and members of public and must also ensure that any captured images do not breach the Data Protection Act 2018.

Users must be aware that geo-location information may be stored within a picture when photographs are taken which may provide the location details of the subject in the photograph, therefore where possible the geo location feature of the phone should be switched off.

Wherever possible personal devices should not be used to take photographs for work purposes.

Any captured images should be transferred to an appropriate Council system (such as EDRM or a shared drive) as soon as possible.

Council mobile devices should only be connected to other Derbyshire County Council issued devices or equipment which have been configured by the ICT Service.

9 Faults, Issues, loss, damage, theft and change of user

Any faults or issues relating to the allocated corporate mobile device, or additional equipment, should be reported to the Service Desk or via Service Desk Online as soon as possible.

If a Mobile device is lost or stolen it must be reported at the earliest possible opportunity to your Manager. You must also report the loss to the ICT Service Desk promptly in order to ensure that the device is remotely wiped and disabled via the Mobile Device Management System (MDM). A security incident must also be raised via Halo.

10 Google Managed Play Store

The Google Managed Play Store is Derbyshire County Council's private Application Store which is where the Council publishes approved applications for employees to download onto their mobile devices.

The downloading and use of additional software, facilities, programs or apps to mobile devices is not permitted unless the software has already been approved by Derbyshire County Council and has been placed in the Company Portal.

Security measures installed on any mobile device should not be changed or deleted.

11 Tethering

Tethering is linking a Laptop or other device to a mobile device in order to obtain internet connectivity via the Mobile Network.

Although staff are able to tether their mobile device to their laptop should the need arise – this should not be normal operating procedure where DCC network or WiFi is available.

12 Responsibilities

All users have a duty to abide by all Council policies and procedures to ensure the safe, secure handling of all electronic data.

13 Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Council assets, or an event which is in breach of the Council's security procedures and policies.

All users have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Council's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Council.

In the case of third-party vendors, consultants or contractors non-compliance could result in the immediate removal of access to the system. If damage or compromise of the Council's ICT systems or network results from the non-compliance, the Council will consider legal action against the third party. The Council will take appropriate measures to remedy any breach of the policy through the relevant frameworks in place. In the case of an employee then the matter may be dealt with under the Council's disciplinary process.

14 Glossary of terms

Geolocation – in the case of Mobile devices, it is the ability to identify of the actual real-world location of an object that has be photographed/videoed.

Near-Field Communication – wireless communication protocol between two electronic devices over a short distance (up to 4 cm)

Bluetooth - wireless communication protocol between two electronic devices over a short distance (typically up to 10m)

This document is owned by the Information Governance Group and forms part of the Council's ISMS Policy and as such, must be fully complied with.