Bring Your Own Device (BYOD) Acceptable Use Policy (AUP)

1 Version History, details and author

1.0	Andrew Murley	14/10/2020	Draft – for Head of Service, ICT Organisational Management
2.1	Andrew Murley	01/02/2021	
2.2	Andrew Murley/Mez Demarais	05/02/2021	Reviewed and reflected comments from Enterprise Architecture
2.3	Andrew Murley/Mez Demarais	15/03/2021	Reviewed and reflected comments from Server Management
2.4	Andrew Murley	14/04/21	Draft considering latest comments and CE+ requirements.
2.5	Rob Pearson	26/05/2021	Comments made prior to feedback.
3.0	Rob Pearson	08/06/2021	Approved by Information Governance Group.
4.0	Jo White	09/07/2024	Reviewed by Information Governance Group.
5.0	John Allen	12/08/2025	Minor changes to include remote wipe and named Web Browser.
6.0	John Allen	09/12/2025	Approved by Information Governance Group. Mandatory MFA added.

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

A.5.10 - Acceptable Use of information and other associated assets
A.5.14 - Information transfer
A.5.15 - Access control
A.6.7 - Remote working
A.7.9 - Security of assets off-premises
A.8.1 - User endpoint devices
A.8.7 - Protection against Malware

2 Introduction

The Council is committed to flexible working arrangements and recognises the benefits of using privately owned devices to access its information and resources. This policy identifies the responsibilities of the device owner to ensure Council systems, resources and data are appropriately protected.

There are security risks associated with using personal devices and it is vitally important that the use of these devices does not compromise the Council's information and/or systems and that data remains protected should devices be lost, stolen, used by another person, or compromised in a security breach.

3 Purpose

The purpose of this policy is to ensure that personally owned (BYOD) devices (e.g. laptops, tablets and smart phones) used to access the Council's data/information and systems are appropriately secured and used in accordance with the Council's requirements as identified within this policy.

4 Scope

The scope of this policy applies to all employees, elected members, contractors, volunteers, apprentices, student/work experience placements, partner agencies, agency staff and third parties.

All parties must have prior agreed, authorised access to any Council administered/hosted/licensed software, digital resources, networks, servers and infrastructure together with communication channels and the data/information stored or carried thereon.

5 Policy statement

The Council needs to ensure that its systems, networks and data as well as the information entrusted to it by individuals, statutory organisations, third parties, agencies and government departments are appropriately protected.

<u>Owner responsibilities and supported devices:</u>

- Access for BYOD owners must be through Microsoft 365 (office.com) and the Cloud via the Microsoft Edge Browser only to authorised applications and data, as available under a user's Council profile via their authorised credentials.
- Access for BYOD owners through Microsoft 365 (office.com) must be competed using Multi Factor Authentication (MFA) which is mandatory for all employees, elected members, contractors, volunteers, vendors, agency staff and partners accessing organisational resources.
- Users must register for MFA prior to being granted access to any Council Digital resources
- Refusal to register and adopt MFA could result in access to Council digital resources being denied.

- Exceptions for use of MFA are not permitted unless explicitly approved by the Council Senior Information Risk Owner (SIRO) and documented with compensating controls.
- Each device must be on the latest stable release of its operating system software and each local application (if used) must also be on the latest stable release.
- Any device which is modified against the manufacturer's recommendations must not be used.
- A minimum of a 6-digit pin or biometric is required to access the device.
- If you wish to use your personal device to access Council information and systems, and you are unsure how to do this, please contact the Digital Services Service Desk or your departmental Digital champion in the first instance.
- You must ensure your device is kept up-to-date regarding all/any specific manufacturer device or software updates/patches. This is a requirement to connect to the Council's systems and must be adhered to. It is strongly recommended that all auto updates are enabled for device Operating Systems.
- You must ensure any security software, on the device is kept up-to-date. This is a requirement to connect to the Council's systems and must be adhered to. It is strongly recommended that all auto updates are enabled for the device's Security Software.
- It is the responsibility of all parties identified in the scope of this policy to comply with the Council's Information Security Policies when using their own device.
- Authorised access to corporate systems, applications and data will be available via a remote view only, with no information persisting locally. It is the user's responsibility to ensure local files are deleted from their personal device after each use, e.g. downloads folder, pictures etc.
- In accordance with the Council's Mobile Working Procedures;
    - downloading of the Council's files, documents and information classified as 'Restricted' or 'Controlled' or any other confidential or sensitive type of Council data to the device must not be performed by the user.
    - Saving of 'Restricted' or 'Controlled' or any other confidential or sensitive type of Council information, other than to corporate authorised storage, must not be performed by the user.
- You are responsible for protecting the device and must not assist anyone with accessing the Council's information or systems using your device.
- The device should be able to be remotely wiped or deleted and configured to do so by the user
- The device must have disk encryption enabled to protect "data at rest"
- Prior to selling, recycling, giving away or disposing of your device, you are responsible for ensuring that any information stored on the device is removed and that the device is wiped or factory reset in a way that removes all configuration and data. Council information must not be stored or remain on the device.
- Information classified as 'Restricted' or 'Controlled' or any other confidential or sensitive type of Council information, must not be screenshotted or printed, unless in exceptional circumstances. Printing and taking screenshots is allowed only for information classified as 'Public'.
- You must inform the Digital Services Service Desk immediately should the device be stolen, lost, you suspect a data breach, or consider Council information has been mis-used or shared accidently or inappropriately.

- Any private or personal information, including applications relating to you on the device, are entirely your own responsibility. You are responsible for the safekeeping of your own personal data.
- When using a personal device to access Council information and systems for work related purposes, you are responsible for protecting that device and are expected to behave in an ethical manner in accordance with the Council's policies and procedures.
- The Council recommends that you insure your device and to advise the insurer that it could be used for work related purposes.

Council responsibilities:

- The Council acknowledges that it is responsible as a Data Controller for ensuring data under its control is protected and remains compliant in accordance with the Data Protection Act (2018) and the UK General Data Protection Regulation.
- The Council reserves the right to deny access to Council data and systems for specific users or from specific devices if the standards identified in this policy are not met.
- The Council is not responsible for the loss, theft or damage to a personal device whilst being used for Council business.
- The Council is not responsible for any costs incurred resulting from the use of personal devices for Council business purposes.

Digital Services responsibilities:

- Digital Services will manage the personal device access - ensuring only suitable devices connect and that appropriate security is in place for that connection, as far as this is possible with current Mobile Device Management tooling.
- Digital Services will maintain and publish the minimum list of requirements herein in order for personal devices to be allowed to connect.
- Digital Services will ensure users who have left the Council or who are no longer authorised, will no longer have the ability to use personal to access its systems and data – for employees leaving the Council, this will be in accordance with the starters and leavers process.
- Digital Services will immediately restrict any personal device that does not meet or has contravened the required security standards, as far as this is possible with current Mobile Device Management tooling.

Information incidents and monitoring:

In accordance with the Council's 'Security Incident Management Policy and Procedures', which you are required to comply with:

- You are required to notify the Council via Halo of any information security incident or breaches involving the use of personal devices – providing all relevant information and details. Digital Services will then work with the relevant manager to advise of any further required action.
- Additionally, dependent on the severity of any Information security incident, your personal device access to Council systems and data may be immediately restricted.
- The Council will not monitor the private usage of any personal device.
- The Council has the right to inspect any device you are using for work use, through a request from your line manager, a member of Digital Services or from Audit Services.

- Council information held on personal devices may be subject to FOI and EIR requests.
- The Council will ONLY check on the compliance of that device against the stipulations laid down in this policy and will not investigate any other usage or data.
- Any data or information misuse or data breach inadvertently observed through this inspection will be recorded and managed accordingly.
- Refusal to submit your device for such an inspection in a timely manner may lead to disciplinary action, or treated as a data breach and managed accordingly.

6 Microsoft 365 Applications

The Council permits the use of personal devices to access Microsoft 365 applications, such as Outlook and Teams.

The process for getting your personal device set up to use Microsoft Applications is;

1. Set up Multi-Factor Authentication (MFA) for your DCC Microsoft account. The authenticator app is the Microsoft recommended tool.
2. Download relevant O365 app (outlook/teams etc) or access via the web.
3. Sign into the web-based client or the downloaded app.
4. Input your login/credentials
5. MFA prompt appears
6. Successfully pass MFA
7. You can now access the O365 service from your own device.

7 Council Business Systems

The Council does not recommend using personal devices to access the council's business systems. A Council managed device should always be the first choice.

Personal devices should only be used in exceptional circumstances as determined by Departmental Senior Management with reference to the Information Governance Group. If personal devices are deemed to be necessary it is preferable to access the required systems by using a virtual desktop.

Personal devices must have up to date software and antivirus.

Council information must not be intentionally saved or stored on personal devices. Temporary downloads created by apps or browsers may occur; these should be deleted as soon as reasonably practicable once identified.

After using a personal device to access council systems the user should delete items in the downloads folder.

8 Exclusions

Council owned and provisioned devices which will already have the required security standards incorporated.

9 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 Council employees, elected members, partner agencies, contractors, volunteers, apprentices, student/work experience placements and vendors 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

The Council will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process and or legal action.

The Council's Security Incident Management Policy and Procedures can be found using the link below.

All users of the Council's ICT facilities must comply with this policy and be aware of the Council's Information Security Policy

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.