Use your Own Device (UYOD) – Office 365 Standard

Implementation date: 23rd June 2020

Control schedule

Approved by	Cyber and Information Security Steering Group
Approval date	23rd June 2020
Senior Responsible Officer	Deborah Smart, Executive Director Corporate Services
Author	Mike Brown – Cyber Security Manager
Scheduled for review	October 2024

Version control

Version	Date	Author	Comment
1.0	23/06/2020	Mike Brown	Approved by CISSG
1.1	01/09/2021	Mike Brown	Review
1.2	01/09/2022	Mike Brown/Mark Burtenshaw	Annual review
1.3	05/10/2023	Mike Brown/Mark Burtenshaw	Annual review
1.4	10/10/2024	Mike Brown/Mark Burtenshaw	Annual review

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

Use your Own Device (UYOD) – Office 365 Standard

Contents

1. Introduction
2. Purpose
3. Supported Devices
4. Available Services
5. Approval Process
6. Device Owner Responsibilities
7. City of Edinburgh Council Responsibilities
8. ICT Responsibilities
9. Security Incidents
10. Monitoring
11. Appendix – Relevant policies
12. Appendix - Release of Liability and Disclaimer
13. Glossary

Introduction

1.1 The City of Edinburgh Council (the Council) supports the use of personal devices such as laptops, smartphones and tablets to enable access to Council information for work purposes to the standard set out in this document. Using a personal device in this way is called Use Your Own Device (UYOD). This standard relates to UYOD using M365 products (Microsoft) accessing Corporate M365 services.

1.2 It is not a requirement to use personal devices for work purposes, but where utilised, all users must adhere to the terms of this policy and must also comply with the Council's ICT Acceptable Use Policy, which can be found at this link: https://orb.edinburgh.gov.uk/downloads/download/6398/ict_acceptable_use_policy

1.3 There are increased information risks associated with UYOD, such as making sure that Council information is kept secure even if your personal device is lost or stolen or used by another person.

Purpose

2.1 This standard is intended to reduce the risks of UYOD by clearly outlining individual responsibilities, minimum requirements, and acceptable use.

2.2 This standard allows full use of online M365 services but does not allow data to be downloaded to personal devices. Other controls exist to monitor and prevent such downloading.

2.3 This standard is for all employees, Elected Members, workers (e.g. casual workers or agency staff), contractors and third parties who access the Council's information using a personal device.

2.4 Breach of this policy, the ICT Acceptable Use Policy, or any other applicable Council standard may result in loss of UYOD access. Possible action may be taken in response to a breach, including:

2.4.1 In respect of council employees, potential disciplinary action, including potential dismissal in cases determined as gross misconduct;

2.4.2 In respect of casual workers, agency workers, contractors or third parties, potential termination of the engagement, with or without notice; and

2.4.3 In respect of Elected Members, consideration of whether such an incident constitutes a breach of the Code of Conduct for Councillors and, if necessary, warrants a referral to the Standards Commission for Scotland.

Supported Devices

3.1 Devices still under vendor supported versions of Windows, Android, macOS, iPadOS and iOS (Apple) are acceptable for UYOD at the Council. Windows and macOS access will be web only. Current anti-virus and firewall services must be present and up to date on devices where applicable.

3.2 Other devices that are non-vendor supported by Windows, Android, macOS and IOS (Apple) are not supported for UYOD, because they do not meet the required security standards.

3.3 Rooted or jail-broken devices will not be enabled for UYOD use. Any device that becomes rooted or jail-broken that enables access to Council systems as part of this standard will have access denied or removed.

3.4 Any compliant device requiring access to the Council M365 Tenant will be required to register with Azure AD before full access is granted. For devices connecting via a web browser, controlled restricted access may be provided without registration with Azure AD

Available Services

4.1 The services available for UYOD will depend on current technology and network constraints.

4.2 Some services may be restricted by the constraints of your personal device or might require additional apps to be downloaded. A maximum of two concurrent sessions (e.g. using laptop and iPhone at the same time) will be permitted to a single user / device. (Access to M365 services can be obtained simultaneously on two devices.)

4.3 Details of the currently available services can be found on the myICT Orb (intranet) pages.

Approval Process

5.1 M365 applications are available to anyone to use on their own device but a Council active directory account and M365 licence is required to access Council data and application features.

Device Owner Responsibilities

6.1 If you use your personal device to access Council information, you will be responsible for protecting the device. You must ensure the device is not used by anyone else to gain access to Council information – even if you think the information is not confidential.

6.2 Device owners must behave in accordance with Council policies while using personal devices in the course of their employment with the Council.

6.3 It is mandatory that you set a pin of at least six numbers, or equivalent biometric/pattern lock feature, to unlock your phone as a minimum.

6.4 As the device owner, you have some specific responsibilities, **you must**:

a. Be aware that no other user of the UYOD device is authorised to access Council information services. The use of separate password protected profiles is recommended if the device is shared (Laptop, Desktop, Phone, or Tablet). Automatic lock policy of no longer than five minutes should be enforced, and a password or biometric/pattern control is required to unlock.

b. Perform a full device factory reset prior to disposal/sale of your device. This ensures Council information is removed securely.

c. Be aware that any private information or applications on the phone are entirely your own responsibility.

d. Adhere to Council policies for working practice and information security when you use your personal device for UYOD.

e. Always take appropriate steps to maintain the security of Council information.

f. Not attempt download of Council information or files to your mobile device.

g. Ensure that your device is compliant, ensure auto updates are switched on, and that security software is up-to-date. If your personal device no longer meets the minimum requirements required to access Council information securely, access will be removed automatically.

h. Report the loss or theft of your personal device to Digital Services (CGI) immediately by phoning 0800 085 7232. Digital Service (CGI) will remotely remove access to Council information.

i. If you think that your access to Council information has been misused, or that Council information has been accessed or shared inappropriately, you must notify Digital Services (CGI) immediately by phoning 0800 085 7232. Digital Services (CGI) will remotely remove access to Council information and notify our Information Governance Team.

j. You are responsible for the safekeeping of your own personal data.

k. You will be responsible for paying any network charges you incur whilst using your personal device for UYOD.

l. You should use your phone in an ethical manner. Any device which is found to be jail-broken, rooted, or otherwise modified beyond the routine installation of updates as directly provided by the manufacturer or mobile operator will automatically lose access to Council systems.

6.5 Any personal device used at work may be subject to 'discovery in litigation'. This means that it could be used as evidence in legal action raised by, or brought against, the Council. Your data could be examined not only by the Council but also by other parties in any legal action.

City of Edinburgh Council Responsibilities

7.1 As a data controller, the Council is responsible for ensuring that all processing of personal data which is under its control, remains in compliance with the General Data Protection Regulation (UK) and the Data Protection Act 2018.

7.2 The Council will respect the privacy rights of individuals and only implement security measures which are required to meet its obligations as a data controller.

7.3 The Council will not be responsible for covering the costs of damage to, or loss of, any personal device used for UYOD.

ICT Responsibilities

8.1 Digital Services and or CGI will manage the UYOD facility, ensuring appropriate security is in place, and that only suitable devices can connect.

8.2 Digital Services and or CGI will not be responsible for supporting or maintaining any personal device used for UYOD. They will maintain and publish a list of minimum requirements, and available services.

8.3 Digital Services and or CGI may remove access from personal devices which have not connected to The City of Edinburgh Council for more than 30 days. Device access may also be removed in the event of a user leaving the Council (employee, Elected Member, worker (e.g. agency), contractor and third party).

Security Incidents

9.1 In the event of the theft or loss of a device, or data compromise (an "information incident"), you must inform Digital Services (CGI) Service Desk immediately by phoning on 0800 085 7232. Failure to do so may result in action being taken, including:

9.1.1 in respect of council employees, potential disciplinary action, including potential dismissal in cases determined as gross misconduct;

9.1.2 in respect of casual workers, agency workers, contractors or third parties, potential termination of the engagement, with or without notice; and

9.1.3 in respect of Elected Members, consideration of whether such an incident constitutes a breach of the Code of Conduct for Councillors and, if necessary, warrants a referral to the Standards Commission for Scotland.

9.2 Digital Services (CGI) will work with the Information Governance Unit to manage the information incident as required. If personal data has been compromised as a result of the incident, the Council's data protection breach procedure should be followed. The Information Governance Unit will be able to support and advise you in relation to appropriate action to take to address the situation.

9.3 Depending on the severity of any information incident, Digital Services and/or CGI may immediately restrict your UYOD access to Council systems in order to manage the incident appropriately.

Monitoring

10.1 UYOD access will be automatically monitored to ensure that personal devices are kept up-to-date and are secure. Any personal device which does not meet security requirements will have UYOD access remotely removed.

10.2 In the event of any misuse of UYOD access, HR and relevant line managers will be notified accordingly.

10.3 The Council cannot and will not monitor the private usage of your phone.

Appendix – Relevant City of Edinburgh Council Policies

- ICT Acceptable Use Policy
- Disciplinary Procedure
- Health and Safety Policy

Appendix – The City of Edinburgh Council release of Liability and Disclaimer

12.1 The Council hereby acknowledges that the use of a personal device in connection with Council business carries specific risks for which you, as the device owner and user, must assume full liability. These risks include, but are not limited to, the partial or complete loss of data as a result of a crash of the operating system, errors, bugs, viruses, and/or other software or hardware failures, or programming errors which could render a device inoperable.

12.2 The Council hereby disclaims liability for the loss of any such data and/or for service interruptions. The Council expressly reserves the right to delete from your device the

management application (or similar applications) at any time as deemed necessary for purposes of protecting or maintaining the Council's infrastructure and services.

12.3 The Council also disclaims liability for device owner injuries such as repetitive stress injuries developed. The Council provides IT equipment that is suitable for long-term office use. Device owners bring and use their own devices to use at the Council at their own risk. Device owners are expected to act responsibly with regards to their own device, keeping it up to date and as secure as possible. It is their duty to be responsible for the upkeep and protection of their device.

12.4 The Council is in no way responsible for:

a. Personal devices that are broken while at work or during work-sponsored activities.

b. Personal devices that are lost or stolen at work or whilst undertaking work-related activities.

c. Maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues).

d. The management or creation of users' own 'cloud-based' user accounts, which are required for purchasing software, or backing-up personal data.

12.5 The Council does not guarantee that service will be compatible with your equipment, or warrant that the service will always be available, uninterrupted, error-free, free of viruses or other harmful components, or will not damage your device, although it shall take reasonable steps to provide the best service it can.

12.6 Furthermore, depending on the applicable data plan, the software may increase applicable rates. You are responsible for confirming any impact on rates because of the use of Council-supplied applications as you will not be reimbursed by The City of Edinburgh Council.

12.7 Finally, the Council reserves the right, at its own discretion, to remove any Council-supplied applications and any associated data, including cached or encrypted data stored by the Council-supplied applications, from your personal device because of an actual or deemed violation of the Council's UYOD standard or change or revision of Council standard on UYOD.

Glossary

Rooted or Jail-broken – Jail-broken or rooted devices are devices that have been adapted to give unrestricted or administrative access to the mobile device's entire file system.

Use Your Own Device - Use your own device (UYOD) means being allowed to use your own personal device, rather than being required to use an officially provided one.

GDPR UK - The Data Protection Act 2018 is the **UK's implementation of the General Data Protection Regulation** (GDPR). Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is: used fairly, lawfully and transparently

M365 - Microsoft 365 is a Software as a Service (SaaS) solution that includes Microsoft Office and other services, such as email and collaboration, from Microsoft's cloud server

M365 Tenant - For our purposes, a Tenant is a term used for an Office 365 Organization.

Windows, Android, iPadOS, iOS and macOS - Windows is a product of Microsoft, Android is developed by Google, and iPadOS, iOS and macOS are Apple products

Vendor Supported – The manufacturer of the device is still providing software and security updates