Bring Your Own Device (BYOD) Policy

Approved by Committee on
DATE with an implementation date of 1st October 2019

ABERDEEN
CITY COUNCIL

Control Document

Approval Date: -	Committee Date
Implementation Date	1st October 2019
Policy Number	
Policy Author(s) and Owner	Chris Sellar, **Policy Author** Andrew Howe, **Policy Owner**
Approval Authority:	Operational Delivery Committee
Scheduled Review:	Annually
Changes:	Policy Creation

Contents

1. Purpose Statement

This policy outlines the Council's position on using personal devices to access Council information, data, systems/applications and any other ICT resources. This is often referred to as Bring Your Own Device (BYOD).

For the avoidance of doubt, the system(s)/application(s) refers to any Council administered/hosted/licensed software, digital resources, networks, servers and other infrastructure, and communication channels, and includes the data carried and stored thereon.

2. Applicability and Scope Statement

This policy is for all staff, agency staff, elected members, contractors, sub-contractors and third parties who access the Council's information, systems and/or applications using a personal device.

BYOD is not an automatic right; both the person and the device must meet eligibility criteria, and Authorised Signatories must agree that the business case exists for its adoption.

3. Responsibilities

There are several roles and responsibilities that are in place to ensure that BYOD is appropriate and controlled for each business cluster and function. Responsibilities are as follows:

3.1. Directors/Chief Officers

- Decide if BYOD is appropriate within their Function as a whole, or within specific Clusters or Teams.
- Ensure that by approving BYOD for staff in their Service, they will not breach any Regulatory or Statutory obligations, or obligations signed up to in partner Information Sharing Agreements or Memorandums of Understanding
- Decide if it is appropriate to approve BYOD for those listed in the BYOD Eligibility Exception List.
- Notify their Senior Management Team and staff of who is and who is not eligible for BYOD.
- Nominate Authorised Approvers.
- Suspend or terminate BYOD access, or, depending on the severity of the circumstances, suspend or terminate full ICT access in the event of a breach of policy.

3.2. Line Manager

- Assess requests for BYOD access to confirm that the person meets the eligibility criteria and there are no known reasons why it is not appropriate for their request to be approved.
- Authorise requests if approved.
- Ask Digital and Technology Cluster to have a mobile device deregistered once it becomes no longer appropriate for that person to have BYOD access.

3.3. Digital and Technology

- Will approve BYOD use following receipt of an authorised request for an individual or group of individuals, Cluster or Function.
- The BYOD Device Requirements Standard details the minimum requirements that are subject to change (sometimes without notice). Any changes to the minimum requirements will be posted on the Council's intranet or available from the Service Desk.
- Digital and Technology will maintain a list of approved users, and their agreement to abide by this policy when using BYOD.
- Digital and Technology will manage the guidelines and procedures of BYOD in line with this, and any relevant ICT Policies.
- Digital and Technology will ensure that all BYOD management software is kept up to date to protect user's devices.
- Digital and Technology shall ensure that the BYOD architecture is validated on an annual basis by an independent IT Health Check.
- Suspend or terminate BYOD access, or, depending on the severity of the circumstances, suspend or terminate full ICT access in the event of a breach of policy.

3.4. BYOD Users

By making an application for BYOD, users are agreeing to:

- Ensure that any data processed by them using BYOD continues to be for Council business purposes only and in line with the original reason for being collected, in accordance with Data Protection legislation.
- Follow all Council Policy and Guidelines in the same way they would if using Council-owned devices and understand that failure to do so can lead to disciplinary action, as well as legal action, against you as an individual. This is particularly the case for documents supporting this Policy are listed under section 4.
- Meet and comply with the requirements of Eligibility Criteria.
- Follow the Council's guidelines on the use of BYOD in addition to this BYOD Policy.
- Return Council-issued devices to ICT Services if opting to user your own device. Due to the nature of the mobile-device-management technology, it may not be possible for a person to use a Council issued device AND their own device to access their accounts.

4. Supporting Procedures & Documentation

Related Policy Documents Suite

This policy will supplement the following existing Council policies

- Corporate Information Policy
- ICT Acceptable Use Policy
- Employee Code of Conduct
- Corporate Protective Monitoring Policy
- Councillors Code of Conduct (for Elected Members only)
- ICT Access Control Policy

Related Legislation

This policy helps to ensure that the Council offers BYOD in a way which supports its compliance with;

- The Data Protection Act 2018
- General Data Protection Regulation
- The Public Records (Scotland) Act 2011
- The Computer Misuse Act 1990
- The Human Rights Act 1998
- The Regulation of Investigatory Powers (Scotland) Act 2000
- The Health & Safety at Work Act 1974
- The Copyright, Designs and Patents Act 1998
- The Environmental Information (Scotland) Regulations 2004
- The Public Records (Scotland) Act 2011
- The Freedom of Information (Scotland) Act 2002

Supporting Documents

This policy is supported by the following procedures;

- Device Requirements for BYOD Guidelines, ACC
- BYOD Operating Procedures and Guidelines, ACC

5. Policy Statement/s

The Council recognises the benefits of BYOD but also needs to ensure that Council systems, networks and data are appropriately protected. The Council's position is that access to personal devices for work business is only permitted in accordance with the terms of this policy and it's supporting procedure.

5.1. What IT Services are available?

Digital and Technology will maintain and publish a list of current, approved services for Bring Your Own Device. These will be published on the Council's intranet.

In Principle the Council will offer 3 types of BYOD to its ICT users.

- **Unmanaged** - Web access to systems such as email.
- **Managed Apps** - Application Access to Council resources via Mobile Application Management
- **Fully Managed** - Full device management with the Council's via Mobile Device Management

Not all council services will be available for BYOD and users should first consult the approved services list to ensure that it will meet their needs before applying for BYOD.

5.2. What is NOT covered?

The Council will not support or maintain any personal device. Furthermore, the Council will not cover any damage to the devices, loss of personal data that may occur as a result of installing any mobile device management solution or when data is removed as part of the data wiping ability of the solution. The Council makes reasonable endeavours to ensure that your device is not affected and that only Council data is erased, but this cannot be fully guaranteed, and the Council accepts no liability for issues resulting from use.

The Council accepts no liability for any failure of your device or for providing a replacement if damaged. It is recommended that device owners insure their device as part of their home-contents insurance, or via a specific mobile-device insurance scheme, and advise their insurer that the device will be used for work purposes at home and at work locations.

The Council will not permit the use of any personal device out with the scope of this policy and available services.

Use of your own device to access Council data is at your own expense. The Council will not reimburse you for any costs incurred or for any damage to your device caused using Council systems.

6. Definitions

"**BYOD**" – Bring Your Own Device. The term used to describe using a personal device for business use.
"**MDM**" - Mobile Device Management. Full device management, protecting both the device along with the data contained within the device.
"**MAM**" - Mobile Application Management. Application management, protecting the data within certain approved apps to access business data.

7. Risk

7.1. Cluster Risk Registers

Information Asset Owners are responsible for managing risk to the information assets that they are responsible for; these risks are managed through the Functional Cluster Risk Registers. Registers and are included in Business Continuity planning and disaster recovery arrangements wherever appropriate.

7.2. Corporate Risk Register

Information management and security pose a strategic risk for the Council which is recorded in the Corporate Risk Register. Corporate Risk Register is owned by the Chief Officer for Business Intelligence Unit and reviewed monthly at the CMT (Stewardship) meetings.

7.3. Breaches, Misuse and Incident Reporting

All Users are responsible for reporting known or suspected breaches of this Policy immediately to their Line Manager, who should then report the incident to the ICT Service Desk in the first instance. ICT Service Desk will log an Information Security incident.

The Council may, at its sole discretion, suspend or terminate BYOD access, or, depending on the severity of the circumstances, suspend or terminate full ICT access for a User in contravention of this Policy. The Council may take such action as it considers necessary, including taking disciplinary action or disclosing information to law enforcement agencies.

8. Policy Performance

BYOD User uptake and usage will be measured on a monthly basis to ensure that services are delivered to meet Council needs. Key Performance Indicators (KPIs) will be used to focus on uptake and usage by Function/Cluster, Application usage, device types, OS levels are examples of KPI's that will be measured and reported as part of Digital and Technologies KPI.

Any breaches or deviation from this policy will be reported via the Information Security Information Reporting Procedure, and they will be investigated accordingly. These will then be reported in the Information Governance Management Quarterly Performance Report, and by the Council's Senior Information Risk Owner (SIRO) to the Corporate Management Team, as required.

9. Design and Delivery

Technology Principles

Flexible and Agile: We will continually embrace new ways of doing things based on emerging technologies. We will be flexible to change how we do things as the underlying technology and digital capability changes. This will mean looking at things through the lens of how technology can be exploited to unlock further capacity in the system.

Technology will enable our workforce to work from anywhere, with anyone and at any time.

Process Design Principles

Security and privacy by design: In designing a new process, we should engage the appropriate privacy, security, and legal officer(s) to discuss the type of information collected, how it should be secured, how long it is kept, and how it may be used and shared.

10. Housekeeping and Maintenance

This policy does not replace any existing policy and is the first version of Bring Your Own Device.

Several IT systems are directly affected by this policy due to the nature of Bring Your Own Device and any of the Council's applications could be approved for BYOD use, where appropriate. The Enterprise Mobility Suite or Mobile Device Management software is required for the facilitation of BYOD.

11. Communication and Distribution

This policy (along with BYOD procedure guide and device guides along with relevant training guides) will be shared with all partners that make use of or access any Aberdeen City Council ICT networks or systems. The policy will be shared on the Council's intranet. Through the application process of BYOD, users will be asked to accept that they understand the policy and its implications before proceeding to access any services available under Bring Your Own Device.

12. Information Management

The Council cannot see your personal information when you enrol a device. When you enrol a device, you give the Council permission to view certain pieces of information on your devices, such as the device model and serial number. The Council uses this information to help protect the corporate data on the device.

The Council collects systems data about BYOD devices on an ongoing basis. This data may be used by the Council to support an investigation of misuse, fraud, criminal activity or data loss, and/or to disable your device access.

What we can **never** see:	What we can **always** see:
Calling and web browsing history Personal Email Text messages Contacts Calendar Passwords Pictures, including photos and camera roll Files Location data	Device model, such as Galaxy S8 The device manufacturer, such as Samsung Operating system and version, such as Android 8.1 Work-managed-app names, such as Outlook Device owner – your work email address Device name Device serial number and IMEI Last four digits of your phone number
What we **might** be able to see:	
Device storage used/available Network information Installed Application Names	

The Council monitors all activity that takes place through the device management tool such as authentication attempts and application installation requests. 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 BYOD access remotely removed.

The Council monitors all network and internet traffic while connected to its infrastructure, such as Wi-Fi. In the event of any misuse of BYOD access, HR and relevant Line Managers will be notified accordingly.

A full Privacy Notice for BYOD users which sets out exactly how and why a BYOD user's personal information is used and managed as part of applying for, registering, and using BYOD will be given to all prospective BYOD users before they apply and accept the Council's BYOD User Agreement. A copy of this Privacy Notice will be made available on the Council's intranet so it can be referred to by BYOD Users at any time.