Bring Your Own Device Procedure

Procedure Reference Number: IT01a

Effective Date:	June 2025	**Review Date:**	June 2028
P&P Review Group Approval Date:	June 2025	**Related Policy**	IT01
Owner:	Head of ICT Strategy & Development	**Department:**	ICT
Issued To:	☐ Board of Management ☒ All Staff ☐ ET/LT ☐ Head Office Managers ☐ C&S Managers ☐ Department/Other: _____	**Method of Delivery:**	☒ Annual Declaration ☐ LearnPro Individual Sign Off ☐ Board Portal
Stakeholder Consultation	☐ All Staff ☐ Customer Engagement ☐ Union ☐ Employee Voices Group ☐ Head Office Managers ☐ C&S Managers ☐ Department/Other: _____	This procedure will be reviewed every 3 years from the date of implementation or earlier if deemed appropriate. If this procedure is not reviewed within the above timescale, the latest approved procedure will continue to apply.	

Version Control

Date	Owner	Version	Reason for Change
Apr-25	Head of ICT Strategy & Development	1.0	New procedure which supports staff to use their own device at Ark if this is their preference.

Summary of changes

Section	Change
All	New procedure

Contents

1.0 Introduction

Bring your own device (BYOD) is the practice to allow Ark employees to use their own mobile device in the workplace for business use. This means employees using their own smartphone to securely access Ark's systems, applications, and information.

This procedure is in place to protect the integrity of Ark data as detailed within our Data Protection Policy to ensure that it remains safe, secure and under Ark control.

This procedure provides the guidance for employees when using their own device at work.

2.0 Procedure Scope

This procedure applies to the following:

BYOD is offered to all Ark employees who have a device that complies with the requirements and have accepted the responsibilities as within this procedure and Ark's ICT Acceptable Use [IT01] policy.

Managers should request BYOD on behalf of their employees via email to the ICT team. It is at a manager's discretion whether employees can make use of BYOD, while managers also have the ability to request removal of BYOD if devices are being misused.

The devices that can be used as part of the BYOD procedure are:

- iOS (have latest version of the operating system)
- Android (have latest version of the operating system)

Employees must follow software security 'best practice' by ensuring the operating system on their devices is kept up to date. Ark's ICT team can and will monitor operating system versions, and where a potential security risk is identified, will require individual devices to be updated. If this is not possible, BYOD functionality will be removed and employees issued with an Ark device instead.

Employees must agree for a 'Work Profile' to be added to their device. This is a ringfenced section held on personal devices which holds all Ark related software and applications, controlled by Ark's ICT team. Ark's ICT employees will not be able to view or access anything outside of the Work Profile on an individual employee's device.

The Work Profile (Microsoft Intune Company Portal application) allows Ark's ICT team to centrally enrol devices, install and update apps, and remotely wipe access.

As part of this procedure employees will have access to the following Ark systems (where appropriate for their role):

- The full range of Microsoft 365 products associated with the employees account, including email, calendar, Teams, and Ark's Intranet;
- AIMS Care Planning app;
- Web browsing;
- Banking and BACS payment applications;
- HR annual leave system;
- Files & Folders (via OneDrive and SharePoint).

This is a broad list and may be subject to change.

If a personal device is connected to Ark's infrastructure, the user is personally liable for their device and internet charges. Use of personal devices are not eligible for the reimbursement of expenses for hardware or internet costs.

Technical support will be limited to software on personal device and on best endeavours basis.

If an employee uses their own smartphone as part of the BYOD scheme they will not be provided with a mobile phone from Ark. Where employees are expected to be contactable via the phone network, an Ark SIM card, or an e-SIM, with an Ark phone number, will be provided (and paid for) by Ark. Employees should speak to ICT about the benefits and drawbacks in this scenario, and consider whether they are comfortable with this approach.

If an employee decides they no longer want to use their own smartphone for work related purposes, they should inform Ark's ICT team who will wipe all applications from the device, and provide users with an Ark owned smartphone if required.

3.0 Employee Responsibility

Employees wishing to participate in the BYOD scheme and who have a qualifying device must also agree to take responsibility for their own device and how they use it.

Employees Must	Employees Must Not
Keep their passwords secure as per ICT security procedure	Share their device or password
Use Biometric features to secure the device if possible	Make copies of data or take screenshots
Keep their operating system updated	Access systems without authorisation
Be careful who can see their screen when accessing work systems	Save work in unapproved locations or applications
Report lost or stolen devices to ICT service desk as soon as possible after the incident	Link their device to an Ark PC or laptop using Bluetooth or a USB
Be aware of their responsibility for all costs	Connect to Corporate Wi-Fi
Help ICT to conduct spot checks if required	Take photos from the gallery of their device or retain them within their work profile beyond the end of the working day
Inform ICT if they leave employment with Ark	
Have their BYOD device switched on during working hours	
Connect to guest Wi-Fi	

If an employee or manager believes any of the above points have been compromised, they must notify the ICT Team as soon as possible.

The expectation is that employees will use their device in an ethical manner in accordance with the IT Acceptable Use [IT01] Policy and other related policies and procedures.

4.0 Security Requirements

All devices must lock with a PIN (personal identification number) or personal biometric security which is set by the user. The security must lock after a maximum time-out of 5 minutes idle time.

Jailbreaking is the process of removing limitations on iOS, Apple's operating system on devices running it, using software and hardware exploits. Rooting involves gaining access to the root account of a smartphone or computer.

Rooted (Android) or jailbroken (Apple) devices are strictly forbidden from accessing Ark systems.

Devices used for personal use only and not part of the BYOD scheme should not access Ark systems.

Employees access to company data is limited based on user profiles which are defined by the Head of IT Strategy & Development and the ICT Team, and are automatically enforced.

If an employee leaves Ark, all login requirements will be disabled, ensuring that no access is permitted once they leave Ark.

5.0 Security Intervention – Mitigation of Risk

As a last resort, the work profile on the device may be remotely wiped if the ICT Team feel the device could be a threat to Ark or is a data protection risk. The decision to wipe the device can only be made by the Head of IT Strategy & Development, in conjunction with the relevant member of ET.

These scenarios include:

- The employee loses their device;
- The employee leaves Ark and there is risk of that person wilfully harming Ark systems or misusing data;
- The ICT Team detects a data or policy breach or virus, or similar threat to the security of Ark's data or IT infrastructure.

An employee who's using a BYOD device is responsible for notifying their mobile phone carrier if their smart phone is lost/stolen. They must notify the ICT ServiceDesk and their line manager as soon as reasonably possible from the device being lost/stolen (via email or phone call).

6.0 Purchasing a New Device

When considering purchasing a new device, it is highly recommended that employees consult with their manager first and/or a member of the ICT Team on a device that will be suitable for the BYOD scheme. Any devices purchased that are not in line with the standard approved device list may not be allowed to be used as part of the BYOD scheme.

Once a device has been purchased the employee's manager must log a ticket with the ServiceDesk to allow access onto Ark's network.

7.0 Monitoring and Access to Devices

Ark will not routinely monitor personal devices. However, it does reserve the right to:

- Prevent access from a device to Ark corporate networks;
- Prevent a device accessing a particular Ark system;
- Take all necessary and appropriate steps to retrieve information owned by Ark.

8.0 Multi-Factor Authentication

Ark has additional security measures to secure its data and systems and employees will be required to undergo multi-factor authentication.

All employees will need to register for Microsoft Multi-Factor authentication and either use the app on the smartphone / tablet, receive SMS messages or automated phone calls.

Employees are requested to authenticate by using their personal device.

9.0 Disclaimer

Ark acknowledges the use a personal device in connection with Ark business carries risks for which the employee assumes full liability.

These include but are not limited to partial or full loss of data due to:

- Crash of operating system;
- Errors;
- Bugs;
- Viruses;
- Malware;
- Software or handwear failures; and
- Programming errors rendering the device inoperable.

10.0 Data Protection

Ark will at all times respect the confidentiality of customers and use personal information about them in accordance with Ark's Data Protection Policy and Procedures.

11.0 Related Policies, Procedures & Documentation

- IT01 ICT Acceptable Use Policy
- G24 Data Protection Policy
- G24a Information Security and Personal Data Breach Management Procedure

12.0 Training & Monitoring Requirements

12.1 Training

ICT staff will have training appropriate to their needs and to the needs of the organisation as identified on their individual learning plans. Ark will ensure that relevant employees have an awareness of this procedure and receive adequate training to enable them to effectively fulfil their roles and ensure Ark's ICT infrastructure remains safe and resilient.

12.2 Monitoring

Devices accessing the Ark network will be monitored on an active basis by the ICT Team.