



UNCLASSIFIED

MOBILE DEVICE POLICY

POL008

Title:	POL008: Mobile Device Policy		
Created:	11 July 2021	Reviewed:	3 Feb 2022
Version:	1.0	Pages:	Page 1 of 5



Introduction

Introduction

To ensure that Akimbo Core Ltd ("Akimbo") can remain compliant with the compliance standards required by our customers, such as Cyber Essentials, certain restrictions are placed on our use of mobile devices. This policy documents what restrictions are in place.

Scope

This policy applies to all staff of Akimbo, including employees, contractors, temporary staff, volunteers, apprentices, and work experience (collectively "Staff"). This policy applies to all mobile phones and tablets that are issued to Staff by Akimbo.

Failure to comply with this policy may result in disciplinary action, up to and including dismissal without notice for gross misconduct.

Review

This policy is to be reviewed every year or in-line with changes to legislation or compliance requirements.

Title:	POL008: Mobile Device Policy		
Created:	11 July 2021	Reviewed:	3 Feb 2022
Version:	1.0	Pages:	Page 2 of 5



Policy

Personal Devices and “Bring Your Own Device”

Staff must not use personal devices for business purposes, including accessing company data.

Device Security

All mobile devices must be secured by a secure PIN number which must:

- ▶ be at least eight characters long
- ▶ not be based on a predictable pattern, such as 123456

Biometric authentication such as FaceID or TouchID may be used alongside a secure password.

Devices must not be rooted or jailbroken and no other action may be taken on a device which may reduce the security offered.

Mobile devices must have all updates installed within 14 days. This includes updates for the Operating System as well as any installed applications.

Only approved applications may be installed on company devices.

Title:	POL008: Mobile Device Policy		
Created:	11 July 2021	Reviewed:	3 Feb 2022
Version:	1.0	Pages:	Page 3 of 5



Approved Applications

The following iOS Apps are approved for use on Akimbo Core mobile devices:

- ▶ Amazon
- ▶ Audible
- ▶ Authy
- ▶ Google Maps
- ▶ Hotels.com
- ▶ Imaging Edge Mobile
- ▶ InShot
- ▶ Instagram
- ▶ LastPass
- ▶ LinkedIn
- ▶ Microsoft Authenticator
- ▶ Microsoft Teams
- ▶ MiPermit
- ▶ Monzo
- ▶ My O2
- ▶ NHS App
- ▶ NHS Covid App
- ▶ ProMovie
- ▶ PhoneDivert
- ▶ Snow
- ▶ Tapo
- ▶ Tidal
- ▶ Trainline
- ▶ TSB
- ▶ Twitter
- ▶ WhatsApp
- ▶ YouTube
- ▶ YT Studio
- ▶ Yubikey Authenticator
- ▶ Zoom

Exceptions

Any exception to this policy must be approved by a Director in writing.

Title:	POL008: Mobile Device Policy		
Created:	11 July 2021	Reviewed:	3 Feb 2022
Version:	1.0	Pages:	Page 4 of 5



Document Control

Author	Date	Version	Status
Holly Grace Williams	11 July 2021	0.1	Draft
Holly Grace Williams	11 July 2021	1.0	Approved
Holly Grace Williams	3 Feb 2022	-	Reviewed

Title:	POL008: Mobile Device Policy		
Created:	11 July 2021	Reviewed:	3 Feb 2022
Version:	1.0	Pages:	Page 5 of 5