Bring Your Own Device	
Reference: GN11c	Effective date: 23 May 24
Page no: **1** of **2**	Approved: 23 May 24
Last revision May 24	Next revision May 27

Introduction

This policy regards the safe use of personal devices for work-related purposes.

Modern personal devices are capable of accessing and storing data, and running business applications. While the use of personal devices can bring many benefits, and help staff to better do their jobs, it also introduces a risk that data, or access to that data, may fall into the wrong hands due to the loss or improper use of a personal device.

We have taken a decision to allow staff to use their own devices for work purposes. This policy has been developed to ensure that this organisation's data is not put at risk from that use.

Purpose

The purpose of this policy is to:

Provide effective controls to ensure that staff access to our data and any information systems through the use of a personal device is authorised, secure and confidential, in line with our business requirements

Ensure the remote processing of our data is operated in accordance with statutory requirements and relevant guidance

Ensure that any risks associated with personal device based access are recognised, assessed and managed.

Scope

This policy applies to all staff as all staff are authorised to access our data on their personal devices.

Definitions

Personal Data: Information that relates to an identified or identifiable individual, as defined by the Data Protection Act 2018 and the GDPR.

Personal devices: A mobile phone that allows users to store information, use email and install programs. Laptops, desktop computers at home, tablet personal computers.

User: Any person authorised to access organisation name's IT systems and networks remotely.

Encryption: The process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing the key. The result of the process is encrypted information. Password protection is not a form of encryption.

Bring Your Own Device (BYOD): The term used to describe the approach of letting members of staff use their own mobile device for work purposes. For example, an organisation might allow their staff to use their own personal devices to access work e-mail while out of the office, rather than supplying corporate owned devices for that specific task.

User Responsibilities for the Security of Personal devices

Where possible data should be accessed and manipulated on a secure cloud-based system and not downloaded to a personal device.

Users must not deliberately put their authorised personal device at undue risk of being stolen, lost or accessed by unauthorised persons.

Stolen or lost equipment must be reported as soon as possible to insert role responsible here.

Users must not store any personal confidential data on a personal device.

Where available users may connect their personal device to the organisation's guest wireless network to get internet access.

User Responsibility for the Security of Personal Confidential Data and Information

Users are responsible for ensuring that unauthorised individuals are not able to see or access our data or systems via the user's enrolled personal device. Personal device screens should be locked when not actively being used.

The use of personal devices for accessing our data or services in a public area should be kept to an absolute minimum, due to the risk of information being viewed and the theft of an unlocked device.

Data should not be held on a personal device for longer than it is required and should be deleted promptly to reduce the risk of the data being accessed by the wrong person.

Personal confidential data must not be stored on an unencrypted device (NB: Password protection is not a method of encryption and must not be relied upon as such).

Emails containing personal confidential data and other confidential information must not be sent to or from personal email accounts.

Reporting Security Incidents and Weaknesses

Staff are responsible for personal devices and all data held on them. In the event of loss, theft or any data security incidents associated with personal device use, users must inform HR Manager and follow the data breach procedures in our Data Security Policy.

Duties and Responsibilities

The Chief Executive is responsible for ensuring that the organisation complies with the statutory and good practice requirements governing personal device use outlined in this policy and is supported by the delegated management responsibilities outlined below.

All Managers are responsible for ensuring that their staff receive relevant training, guidance and support to understand and adhere to this policy and all appropriate supporting guidance

All staff must ensure that they are aware of their responsibilities for complying with personal device use requirements in accordance with this policy. All staff with authorised personal devices must safeguard our information and report immediately any associated security incidents.

Staff Training

All new staff will receive training in data protection as part of their induction process. Appropriate refresher training will be incorporated into the staff training programme.