Title:	**Mobile Device**			**Doc No:**	IS-POL-002
Author:	M Roberts			**Rev:**	0
Owner:	M Roberts	**Approved:**	C Barley	**Date:**	07/06/2018

Mobile Devices Policy

1.0 Purpose

This document specifies the organisations policy for the use, management and security of all Mobile Devices that may hold organisational information. This policy is an important part of the overarching information management system. The information management system exists to ensure that all those who are authorised to, should be able to easily access all the information they need to fulfil their role.

20. Scope

This policy applies to all:

- Organisation issued Mobile Devices`, and;
- Personally owned Mobile Devices.

That are used to access the organisations information, network or ICT facilities including, but not limited to, organisations information systems, email, organisation managed storage.

This policy applies to all staff and third parties (including but not limited to contractors, agency workers and students) operating on behalf of the organisation or undertaking functions and thereby accessing the above systems or who are provided with organisation issued Mobile Devices. These will hereafter referred to as ‘users’.

This policy only applies to learners if they are carrying out a function on behalf of the organisation.

This policy applies to use of mobile devices for business purposes at all times, both during and outside office hours and whether or not users are at their normal place of work.

This policy prohibits the use of personally owned Mobile Devices to access the organisations information system, networks or ICT facilities including but not limited to information systems, emails and organisation managed storage.

2.1 Definitions

Mobile Devices include, but are not limited to:

- Laptop Computers and netbooks
- Tablet Devices
- Smartphones

- Portable storage such as removable hard drives, USB memory sticks and data cards
- Portable audio visual equipment including data projectors, cameras, etc.

Confidential Information consists of information which, if disclosed or made publicly available could damage commercial of financial interests, privacy, reputation or employability, could cause damage or distress to individuals, cause the organisation to not meet its legal obligations, or damage the organisations reputation. The definition of confidential includes any information which is either labelled 'confidential' or, if not labelled 'confidential' would nevertheless be reasonably regarded as confidential.

Organisational Information means information relating to or connected with the organisations business or affairs whether or not such information constitutes 'confidential' information.

2.2 Changes

This policy does not form part of the terms and conditions of employment and the organisation at its discretion review and amend this policy at any time. Provided that Users are notified of amendments (this can be through internal communications addressed to all staff), then they will be bound by this policy as amended.

2.0 Policy Statement

Protecting the organisations information and facilities

The use of any Mobile Device to process and access the organisations information creates risks including those relating to data protection, virus infection, copyright infringement, unintentional or unlawful compromise of data and even loss or theft of device and / or data. The risks are increased, and are also more difficult to manage, when using personally owned Mobile Devices.

The organisation, and its staff, is require to process, and is committed to processing, all personal data in accordance with the Data Protection Act 1998 regardless of the device used to access the information. Organisational Users are required to keep organisation information and personal data secure. This applies equally to organisational information held on the organisations systems and devices or accessed.

Our organisation reserves the right to refuse to allow access to particular devices or software where it considers that there is a security or other risk to its information or ICT facilities.

Our organisation is the owner of all organisational information and the contents of the organisations systems together with everything which is created on, transmitted to, received on or printed from, or stored or recorded on each Mobile Device, in each case during the course of the organisations business or otherwise on the organisation's behalf.

Monitoring of organisational ICT activity logs (relating to Staff usage) will be carried out.

Mobile Device users are responsible for:

- The security of the organisations information and the device on which the information is held.
- Storing organisational information on Mobile Devices only for as long as necessary
- Deleting organisational information from Mobile Devices when no longer required
- Ensuring (where possible) the device has up to date Operating system and anti-virus protection
- Complying with this policy and related policies

Data Access and Storage

Confidential Information should be stored within and accessed from organisational Information Systems and organisational managed storage to ensure security of and appropriate secure access to the information.

Only store the minimum amount of information necessary (to carry out any required task) on a mobile device. A temporary cache may be held on the device, therefor any confidential information should be deleted from the device as soon as the information is no longer required

Device and Physical security

Mobile Devices accessing the organisations information must have a strong (4 or more alphanumeric characters / patterns) passwords / passcodes / PIN enabled to reduce the opportunity for unauthorised access. Passwords / passcodes / PINs must be kept secure. The device should be set to automatically lock if inactive for 5 minutes or less, or locked manually using Ctrl, Alt and Delete keys.

Mobile Devices used to regularly access/store Confidential Information should be subject to additional protection measures to reduce opportunities for loss or compromise of the information.

Mobile Devices should where possible, have operating system and anti-virus updates enabled. 'jailbroken' or 'rooted' devices of these mobile devices which have otherwise circumvented the installed operating system security requirements (making them vulnerable to compromise) are not permitted to connect to the organisations ICT facilities.

Organisational issued Mobile Devices are configured to standard security and other settings and tariffs before delivery to the user. Any changes required to these settings and tariffs must be requested via ICT services.

Physical Security: Mobile Devices issued by the organisation must not be left unsecured whether on or off the organisations premises. When unattended the device must be locked (password / passcode / PIN protected) and the mobile device should be secured with a recommended 2 barriers i.e. limited access building or office and where possible a locked cupboard.

When an employee leaves or changes mobile device

The devices are the property of the organisation and as such must be returned to IT services upon change of user or termination of employment. They must not be sold, given away or otherwise be disposed of by the user.

If devices are not returned (after a reminder process) the matter will be passed to the Directors for a disciplinary matter. The matter may also be passed to the Police for a consideration of further action or for recovery via civil litigation.

Reporting loss or theft

I the event of loss or theft of any Mobile Device the User must act promptly to minimise the risk of compromise to organisational data by immediately:

- Changing the network log in password and notifying IT services of the incident circumstances.
- Changing any other passwords that may have been used in the device.
- Reporting the theft of a device to the Police
- Reporting loss of mobile phone to network provider