

Saving Faces Bring Your Own Device policy

1. Scope

Bring Your Own Device (BYOD) is the practice of allowing staff to utilise personally owned devices (such as smartphones, tablets or laptops) in the workplace, and to use those devices to securely access the organisation's systems, applications and information. Staff who work from home may use their own devices for work. All staff who are authorised to work from home and use their own device are required to read this policy in full and confirm they understand and will comply with it.

Working from home and the BYOD service includes a range of systems and access may vary by individual depending on the requirements of individual roles. Available work systems include email, calendar, intranet and web browsing, internal web-based systems, rotas and scheduling, communication systems, reporting systems, and clinical systems.

2. Support Devices

Staff who use their own devices must use devices that run on supported Apple, Android or Windows operating system. Staff will be expected to ensure devices are kept updated or risk losing access to some systems. Devices must have anti-virus/malware software, be encrypted, and have passcode or biometric security if available with a timeout to lock automatically after 10 minutes of inactivity. Jailbroken or rooted devices are strictly prohibited. Staff must not circumvent security controls.

3. Responsibilities

3.1. Acceptable Use

Staff may only connect to work systems for the purpose of authorised work. Staff must:

- Access confidential data for a specific work-related requirement
- Keep account logins, passwords and pin numbers confidential
- Be careful who can see your screen when accessing work systems

Staff must NOT:

- Access systems without authorisation
- Save work data in unapproved locations or applications
- Copy work data off the device
- Take screenshots of systems of sensitive information
- Share their device or passwords

3.2. Loss or Damage

Saving Faces will not accept any liability for loss or damage of personal devices and data that are using the BYOD system. Staff must immediately inform admin if:

- Their password has been breached
- Their device gets lost or stolen
- IT systems are not working normally

IT will attempt to remotely wipe or disable the device if a device has been lost and stolen.

3.3. Costs

Staff are solely responsible for all costs associated with:

- Purchasing, running, repairing and replacing their personal devices

- Mobile data or WiFi costs related to BYOD usage

3.4. **Monitoring**

Saving Faces will monitor usage of BYOD devices from time to time including the make and model of devices in use and the version of the operating system currently installed. Spot checks will always be conducted in the presence of the staff member and devices will never be taken away from their owner. Admin can access details on usage of corporate applications via the BYOD policy but cannot access personal application data. In some instances, device location may be collected but this data will only be used if the device is lost or stolen.


Staff must:

- Facilitate admin to conduct spot checks when required
- Keep your operating system updated
- Inform admin if you leave employment

Where operating systems are found to be out of date the staff member will be informed and expected to upgrade to a supported version within 10 working days. Failure to remediate will result in access to BYOD services being withdrawn.

4. **Document Owner and Approval**

The Chief Executive Officer (CEO) is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the DSP Toolkit. This will be reviewed annually.

Name	Iain Hutchison
Signature	
Approval Date	8 th February 2023
Review Date	23 rd June 2023

A current version of this document is available to all members of staff on the Saving Faces website.

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial version	CEO	23 rd June 2021

2	Review SM	SM	23/06/2022
2.1	Added the requirement of anti-virus/malware software in <i>2. Supported Devices</i>	FR	07/02/2023