SNAPS Bring Your Own Device Policy

Version Control
Version 0.1
Date of issue 29.4.19
Date of last amendment 29.4.19

Purpose of Policy

Bring your own device (BYOD) refers to the policy of permitting employees to bring personally owned devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications.

This policy is designed to advise how employees at SNAPS can use their own devices to carry out company work using the SNAPS Office 365 portal and is intended to protect the security and integrity of SNAPS' data.

Acceptable Use

SNAPS employees are permitted to use either their own personal or a company device (where relevant) for the purposes of carrying out work on behalf of the charity. This includes, but is not limited to: emailing, calendar usage, photo storage, storing/accessing contacts, creating, saving and editing documents within Microsoft Office packages (e.g. Word, Excel, Powerpoint, One Drive). All SNAPS data and documentation must be created and saved within the SNAPS Office 365 portal.

Security

When a new employee joins SNAPS they will be issued with their own Office 365 login, using their new SNAPS email address and a given password. At first login this password must be changed to a secure password using at least 6 characters and a combination of upper case and lower case letters, numbers and / or special characters. This password must not be shared with anyone else. All company work must be carried out using this login, and, as above, all data must be saved only within the employee's Office 365 account and SNAPS portal. No SNAPS data or information should ever be saved outside of this account; for example, on the employee's personal drives or devices.

If employment with SNAPS is terminated, either by the employee or the charity, then access for that employee to the SNAPS Office 365 network shall be revoked immediately at the employment end date. No company data should be copied and / or removed from the company portal for use after the end of employment with SNAPS.

In addition to the above security measures employees should ensure that screens are locked when any device is left unattended, and a lock screen is activated after a maximum of 5 minutes when a device is sat in an idle state.

The employee is personally liable for all costs associated with his or her device. The employee assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
If any employee has any concerns regarding this policy, or another employee's use of their personal device, then they should speak immediately with the SNAPS Chief Executive or a member of the Board of Trustees.

User Acknowledgment and Agreement

I acknowledge, understand and will comply with the above referenced security policy and rules of behaviour, as applicable to my BYOD usage of SNAPS services. I understand that business use may result in increases to my personal monthly service plan costs. I further understand that reimbursement of any business-related data/voice plan usage of my personal device is not provided.

Employee Name: _____

BYOD Device(s): _____

_____

Employee Signature: _____

Date: _____