SNAPS YORKSHIRE CIO
BRING YOUR OWN DEVICE POLICY
MAY 2025

BRING YOUR OWN DEVICE POLICY

It is recognised that different categories of individuals involved with SNAPS will have different needs in terms of how they use their own devices for SNAPS' work and hold SNAPS' information, therefore this policy is split into 4 different sections namely:

- Contractors (a person or firm that undertakes a contract to provide materials or labour to perform a service or do a job)
- Employees (a person employed for wages or a salary)
- Trustees (a volunteer on the Board of Trustees, who, as a group, are responsible for governing a charity and direction how it is managed ad run) and
- Volunteers (a person who volunteers their time for free)

Contractors' Bring Your Own Device (BYOD) Policy

Purpose of Policy

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

This policy is designed to advise how contractors at SNAPS can use their own devices to carry out SNAPS' work and is intended to protect the security and integrity of SNAPS' data.

Acceptable Use

SNAPS' contractors are permitted to use either their own personal or a SNAPS 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 sent to a SNAPS staff member to be saved in the Microsoft Office 365 One Drive portal. Once the contractor has finished a piece of work and sent all documentation to the staff member, they must delete all files relating to SNAPS from their own devices. (Exception is made for the Finance Manager who needs to have SNAPS' financial information on their personal drives. The Finance Manager will ensure they have measures in place to ensure SNAPS' information is secure and backed up.)

Security

When starting at SNAPS, Physiotherapists and Swimming Teachers will be given a Charity Log login, using their 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 uppercase and lowercase letters, numbers and / or special characters. This password must not be shared with anyone else. All SNAPS work must be carried out using this login, and, as above, all data must be saved only within Charity Log. No SNAPS data or information should ever be saved outside of this account; for example, on the employee's personal drives or devices. Any unauthorised sharing of logins will result in disciplinary action.

All Physiotherapist and Swim Instructor contractors will access SNAPS' records via Charity Log only on SNAPS' devices and will not store any personal information on their own devices. Other contractors should not have access to SNAPS' confidential data or information and therefore information of this kind should never be saved on the volunteer's personal drives or devices. (Exception is made for the Finance Manager who needs to have SNAPS' confidential financial information on their personal drives). Any unauthorised sharing of logins will result in disciplinary action.

No SNAPS' data should be copied and saved by the contractor for use after the end of their period of employment with SNAPS.

In addition to the above security measures contractors 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 contractor is personally liable for all costs associated with their device. The contractor assumes full liability for risks including, but not limited to, the partial or complete loss of SNAPS' 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 contractor 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.

Employees' BYOD

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 SNAPS' information and applications.

This policy is designed to advise how employees at SNAPS can use their own devices to carry out SNAPS' 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 SNAPS 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 or Charity Log. Charity Log must only be accessed on a SNAPS' device.

Security

When a new employee join's SNAPS they will be issued with their own Office 365 and Charity Log login, using their 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 uppercase and lowercase letters, numbers and / or special characters. This password must not be shared with anyone else. All SNAPS' 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 on Charity Log. No SNAPS data or information should ever be saved outside of this account; for example, on the employee's personal drives or devices. Any unauthorised sharing of logins will result in disciplinary action.

If employment with SNAPS is terminated, either by the employee or the charity, then access for that employee to the SNAPS' Office 365 network and Charity Log shall be revoked immediately at the employment end date. No SNAPS' data should be copied and / or removed from the SNAPS' 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 their device. The employee assumes full liability for risks including, but not limited to, the partial or complete loss of SNAPS' 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.

Trustees' BYOD

Purpose of Policy

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

This policy is designed to advise how Trustees at SNAPS can use their own devices to carry out SNAPS' work and is intended to protect the security and integrity of SNAPS' data.

Acceptable Use

SNAPS' Trustees are permitted to use their own personal device for the purposes of carrying out work on behalf of the charity. This includes, but is not limited to emailing, calendar usage, 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 sent to a SNAPS staff member to be saved in the Microsoft Office 365 OneDrive portal.

All Trustees must delete files and emails relating to SNAPS that are more than 3 months old if they are not currently using that file. (Exception is made to the Chair of the Trustees, Vice Chairs of the Trustees and Treasurer who can hold information for longer periods for the purposes of SNAPS' record keeping.)

Security

Trustees should take care when accessing confidential SNAPS' data or information to keep the information confidential. Confidential files should ideally be deleted after reading/use at Board meetings unless the Trustee has cause to use this information on an ongoing basis as part of their role within SNAPS. Confidential information should not be saved on the Trustee's personal drives or devices. (Exception is made to the Chair and Vice Chairs of the Trustees and Treasurer who can hold information for longer periods for the purposes of SNAPS' record keeping.)

No SNAPS' data should be copied and saved by the Trustee for use after the end of their term with SNAPS.

In addition to the above security measures, Trustees 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 Trustee is personally liable for all costs associated with their device. The Trustee assumes full liability for risks including, but not limited to, the partial or complete loss of SNAPS' 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 Trustee has any concerns regarding this policy, or another employee's use of their personal device, then they should speak immediately with the Chair of the Board of Trustees.

Volunteers' BYOD

Purpose of Policy

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

This policy is designed to advise how volunteers at SNAPS can use their own devices to carry out SNAPS' work and is intended to protect the security and integrity of SNAPS' data.

Acceptable Use

SNAPS' volunteers are permitted to use either their own personal or a SNAPS 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 sent to a SNAPS' employee to be saved in the Microsoft Office 365 One Drive portal. Once the volunteer has finished a piece of work and sent all documentation to the staff member, they must delete all files relating to SNAPS from their own devices.

Security

Volunteers should not have access to SNAPS' confidential data or information and therefore information of this kind should never be saved on the volunteer's personal drives or devices.

No SNAPS' data should be copied and saved by the volunteer for use after the end of their period of volunteering with SNAPS.

In addition to the above security measures volunteers 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 volunteer is personally liable for all costs associated with their device. The volunteer assumes full liability for risks including, but not limited to, the partial or complete loss of SNAPS' 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 volunteer 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.

Drafted: 05/05/2025
Approved By Board: 14/05/2025
Next Review Date: 05/2026