FERNY HILLS STATE SCHOOL

PARENTS AND CITIZENS ASSOCIATION

ABN 74 538 686 839

Technology and telecommunications Policy

How we manage technology and telecommunications

Applies to:	All members, volunteers and employees
Author:	Social Media – Margit Rosenthal
Approval:	FHSS P & C Committee
Date approved:	9 March 2021

This Policy details the requirements for the use and security of all technology and communication devices.

1 Aim

The safe and secure use of technology and telecommunications will:

- enhance the operations of the Ferny Hills Parents and Citizens Association (FHSS P & C).
- assist to protect all assets and personal information; and
- assist with compliance.

1 Scope

This applies to all software, hardware and telecommunication devices such as mobile phones, walkie talkies and telephones. All software, hardware, telecommunication devices and the information stored on them remain the legal property of FHSS P & C at all times. Bring Your Own Devices (BYOD) aren't permitted in the workplace[1].

2 Background

FHSS uses a combination of Microsoft Windows, iOS and Android devices. Microsoft 365 is used to configure, protect and manage the devices. Identity services are provided by Microsoft Azure Active Directory. Data is managed and stored in Microsoft Office 365.

3 Establishing and deactivating user accounts

User accounts are established on a least privilege basis meaning that access to information is on a need to know basis. The table below is indicative of current requirements.

Role	Location	Software	Hardware
Lead Coordinator	OSHC	• QKR • Centrelink • CBA CommBiz • Microsoft Office 365 • Windows 10	• Desktop computer • Printer • iPad • Mobile phone • Netgear • CBA EFTPOS
Tuck Shop Convenor	Tuck Shop	• School Shops Online	• Desktop computer • Printer

[1] This means the FHSS school location.

Role	Location	Software	Hardware
		• Microsoft Office 365 • Windows 10	• CBA EFTPOS
Uniform Shop employee	Uniform Shop	• School Shops Online • Microsoft Office 365 • Windows 10	• Laptop computer • Printer • CBA EFTPOS
President		• Microsoft Office 365 (User)	
Treasurer		• Microsoft Office 365 (User) • MYOB (Admin)	
Vice President		• Microsoft Office 365 (User)	
Secretary		• Microsoft Office 365 (User)	
Vice President (OSHC)		• Microsoft Office 365 (User)	
Vice President (Retail)		• Microsoft Office 365 (User) • School Shop Online (Admin)	
Technology Officer		• Microsoft 365 (Admin) • School Shop Online (Admin) • QKids (Admin)	

The Technology Officer[2] will establish a unique individual user account and password at point of employment (where required for an employee) or commencement (in the case of FHSS P & C Executive Committee members (Executive Committee). This password must be changed at the first logon.

Shared user accounts aren't permitted.

Upon cessation, the Technology Officer will deactivate accounts and reassign licences. In the case of FHSS P & C Executive Committee members, the password will be reset and permissions assigned to the new office bearer.

If a third party (such as an auditor) requires access to software applications, this must be approved by the Executive Committee. It's recommended that any contract with the third party include a confidentiality deed and the requirement to comply with this Policy[3]. If approved, a unique individual user account and password must be established.

3.1 Passwords

The following configuration applies to all passwords for computers and licensed software. Passwords must:

1. consist of at least 8 characters including upper and lower case alphabet, numbers and characters;
2. be unique and strong;
3. allow 5 grace logons; and

[2] The Technology Officer is selected by the FHSS P & C on the basis of expertise to perform the IT functions. This may be a company hired to action this Policy.

[3] Ensure a copy of this Policy is provided upon signing the contract.

4. changed every 60 days.

Example: #H0liDay21, IAmGoingOnA3MonthHoliday!

Passwords must not be:

1. single whole word;
2. familiar to the user and therefore easy to guess e.g. dog's name and persons date of birth;
3. written down, stored or 'remembered' in any system;
4. reused; or
5. shared.

Always change any default password at the first opportunity.

Any suspected compromise of a password must immediately be reported to the Technology Officer.

4 Email

FHSS P & C email is to be used for business purposes only. Emails must not contain defamation, any discrimination or items that are subject to copyright where permission hasn't been obtained to use them.

For security, confidentiality and privacy purposes, emails sent to an FHSS P & C address must not be forwarded to a personal address.

Any instance where a suspected malicious link has been clicked on must immediately be reported to the Technology Officer.

4.1 FHSS email accounts and addresses

FHSS P & C email accounts must be configured using the following convention - *position@fhsspandc.online*[4] The following domains have been registered and configured for security purposes:

- fhsspandc.online; and
- position@fhsspandc.com.au.

4.2 Personal email accounts

Personal email accounts must not be linked to FHSS P & C email accounts in any way. Auto forwarding personal emails to FHSS P & C email accounts is prohibited. This is to avoid the risk of cyber security issues as well as maintain a separation between personal communications and business.

5 Software

5.1 Licensing

Software licences must be managed as an asset. This requires any contracts to be complied with which may include the following:

1) renewal dates;
2) protection of intellectual property or copyright; and
3) user management – numbers of users, passwords and access.

[4] Role of the Secretary – P & C email address, P & Cs QLD Info Place.

If not managed well, penalties may apply increasing the cost of administration to the FHSS P & C.

5.2 Management

All software on devices such as laptops, desktop computers, printers and mobiles must be updated as soon as new versions are available. This will ensure any bugs are fixed and that anti-virus scanning kept up to date for cyber security purposes.

In addition, patching may be required to ensure the safety, security and effective use of software.

5.3 Reporting errors

Any errors when using software must be reported to the software provider. At the time of reporting ask how long the error will take to be fixed to ensure the issue can be followed up if required. Ensure you receive a record of the report and note the date and time it's reported.   Follow this up if it's not fixed within the required timeframe.

6 Software

All software used must be properly licenced and only permitted applications can be installed on FHSS P & C devices.

7 Hardware

Personal hardware such as storage devices, desktop computers or laptops can't be used in an FHSS P & C workplace.

Hardware should be engraved as per Queensland Police guidelines and included in the FHSS P & C Asset Register.

All hardware must be always secured. Examples of security include:

- laptops using a Kensington lock tethered to an unmovable object and the key secured in a separate location;
- fingerprint or password protection on mobile phones and computers; and
- laptops, mobile phones and other portable items locked away when not in use.

All devices must be locked when not in use to prevent third party access to systems and information.

7.1 Portable storage devices

Portable storage devices such as:

- USBs;
- floppy disks;
- CDs; and
- DVDS

are not permitted to be used on any FHSS P & C computers due to the risk of transmitting a virus.

Information about FHSS P & C business including personal and sensitive information about parents, employees and children is not to be transferred or copied to portable storage devices. This is to avoid the loss of information or a breach of privacy. It also maintains the safety and security of those persons associated with operations.

7.2 Faulty devices

Any device that isn't working should be reported to the Leader of the area to enable it to be fixed or replaced.

Any requirement for a new device to be purchased must be referred to the Executive Committee.

8 Cyber security

Good cyber security practices are key to preventing cyber attacks. As the frontline of operations, employees and the Executive Committee must commit to actively managing their security practice in their day to day work. Some aspects include:

- only click on legitimate email links – if you're unsure contact the Technology Officer;
- report all security events;
- run anti-virus software regularly;
- log out of systems when not in use for long periods e.g. overnight; and
- ensure your screen is locked when unattended and your computer is secured.

9 Use of cloud

Only permitted cloud services with appropriate security controls can be used. Security controls include:

- prevention of access to data by third parties;
- loss of data;
- physical and environmental security; and
- cloud service provider security policies and procedures and management.

If an external vendor requires an additional cloud service to be used in conjunction with their services, this must be first approved by the Executive Committee.

At all times FHSS P & C must retain ownership of information when using a cloud service.

The use of iCloud, which is standard with Apple devices, is not permitted.

10 Process in case of theft

If a device is stolen, then it must be reported to the Executive Committee. The device will then be remotely wiped using Microsoft Intune and the theft reported to Queensland Police providing the details from the asset register.

11 Disposal of devices

When disposal of a device is required, the device will have a factory reset performed on it and then in the case of a Microsoft Windows device, low level format performed on the device. All data will be retained in Microsoft 365 OneDrive for Business cloud storage for record retention purposes.

12 Risks

	Risk	Controls	RACI
1.	There is a risk that technology is not managed appropriately and information is released or accessed by unauthorised parties.	a) Password configuration is set on all computers and licensed software as per the Policy.	R – Executive Committee A – Technology Officer C and I – Employees and Executive Committee
		b) Technology management practices are reviewed in line with operations and changes in this Policy.	R – Executive Committee A – Technology Officer C and I – Employees and Executive Committee
2.	There is a risk that FHSS P & C technology assets aren't managed and secured resulting in financial loss and operational impacts.	a) Technology assets are managed in line with operations and changes in this Policy.	R – Executive Committee A – Technology Officer C and I – Employees and Executive Committee
		b) Physical controls are in place to ensure technology assets are secured when not in use.	R – Executive Committee A – Employees and Executive Committee C and I – Employees and Executive Committee
3.	There is a risk that users may use another person's individual user account or password	a) FHSS Code of Conduct prohibits this under a duty of care.	R – Executive Committee A – Executive Committee C and I – Employees and Executive Committee
4.	There is a risk that a cyber attack is instigated resulting in a loss or disclosure of personal information	a) Anti-virus software is regularly used. b) Employee cyber security awareness and actions such as reporting.	R – Executive Committee A – Employees and Executive Committee C and I – Employees and Executive Committee

Legend	
R	Responsible
A	Accountable
C	Consulted
I	Informed

13 Business continuity

All files are located on OneDrive for Business. This maintains business continuity by enabling continued access to files securely stored in the Microsoft 365 cloud.

Refer also to sections 8, 9 and 10 for business continuity strategies.

All third party provider contracts must have service level agreements (SLA) identifying and ensuring business continuity.

14 Record keeping

Recordkeeping is the efficient and systematic control of the creation, receipt, maintenance, use and disposal of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records. It is auditable.

Records must be kept as per the Record Retention Schedule[5].

Records can only be deleted or disposed of by following the retention and disposal schedule.[6]

Any attempt to delete or dispose or actual deletion or disposal of records without following the proper processes will be considered a malicious action and disciplinary action will be taken.

15 Disciplinary action

Any action contrary to this Policy will be investigated and may result in disciplinary action including (but not limited to):

- removal of access to systems;
- return of hardware;
- reporting of criminal actions;
- legal action; and/ or
- termination of employment or membership of FHSS P & C.

16 Approval

Any changes to this Policy must be approved at a FHSS P & C meeting.

17 Review

This policy will be reviewed upon any material change in operational practices or *Related documents*. Otherwise it will be reviewed triennially.

18 Related documents

1) Code of Conduct – P & C Association Ferny Hills State School
2) FHSS P & C Asset Register
3) Queensland Government Retention and Disposal Schedule
4) Executive Role – Secretary

[5] Queensland Government Retention and Disposal Schedule.

[6] Queensland Government Retention and Disposal Schedule.