St Francis of Assisi OSHC
Out of School Hours Care Program
312 Childs Road, Mill Park
Phone: (03) 9407 3170
ABN No. 77 054 042 361

INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

Quality Area 7

PURPOSE

This policy will provide guidelines to ensure that all users of information and communication technology (ICT) at St Francis of Assisi OSHC or on behalf of St Francis of Assisi OSHC.

- understand and follow procedures to ensure the safe and appropriate use of ICT St Francis of Assisi OSHC, including maintaining secure storage of information
- take responsibility to protect and maintain privacy in accordance with the service's *Privacy and Confidentiality Policy*
- are aware that only those persons authorised by the approved provider are permitted to access ICT at the service
- understand what constitutes illegal and inappropriate use of ICT facilities and avoid such activities.
- understand and follow professional use of interactive ICT platforms, such as social media *(refer to Definitions)* and other information sharing platforms *(refer to Definitions).*

POLICY STATEMENT

VALUES

St Francis of Assisi OSHC is committed to:

- professional, ethical and responsible use of ICT at the service
- providing a safe workplace for management, educators, staff and others using the service's ICT facilities and information sharing platforms
- safeguarding the privacy and confidentiality of information received, transmitted or stored electronically
- ensuring that the use of the service's ICT facilities complies with all service policies and relevant government legislation
- providing management, educators and staff with online information, resources and communication tools to support the effective operation of the service.

SCOPE

This policy applies to the approved provider or persons with management or control, nominated supervisor, persons in day-to-day charge, educators, staff, students, volunteers, at St Francis of Assisi OSHC. **This policy does not apply to children**. Where services are using ICT within their educational programs, they should develop a separate policy concerning the use of ICT by children.

This policy applies to all aspects of the use of ICT including:

- desktop top computers, laptops/notebooks, tablets, iPads, smartphones
- copying, saving or distributing files
- electronic bulletins/notice boards
- electronic discussion/news groups
- electronic mail (email)
- file sharing
- file storage (including the use of end point data storage devices – *refer to Definitions*)
- file transfer
- instant messaging
- internet usage

- online discussion groups and chat facilities
- portable communication devices including mobile and cordless phones.
- printing material
- social media *(refer to Definitions)*
- streaming media
- subscriptions to list servers, mailing lists or other like services
- video conferencing
- viewing material electronically
- weblogs (blogs)

RESPONSIBILITIES	Approved provider and persons with management or control	Nominated supervisor and persons in day-to-day charge	Educators and all other staff	Parents/guardians	Contractors, volunteers and students
Ensuring that the use of the service's ICT complies with all relevant state and federal legislation *(refer to Legislation and standards),* and all service policies *(including Privacy and Confidentiality Policy and Code of Conduct Policy)*	√	√	√	√	√
Managing inappropriate use of ICT as described in *Attachment 2*	√	√			
Providing suitable ICT facilities to enable educators and staff to effectively manage and operate the service	√	√			
Authorising the access of educators, staff, volunteers and students to the service's ICT facilities, as appropriate	√	√			
Providing clear procedures and protocols that outline the parameters for use of the service's ICT facilities both at the service and when working from home *(refer to Attachment 1)*	√	√			
Embedding a culture of awareness and understanding of security issues at the service	√	√	√	√	√
Ensuring that effective financial procedures and security measures are implemented where transactions are made using the service's ICT facilities, e.g. handling fees, invoice payments, and using online banking	√	√			
Ensuring that the service's computer software and hardware are purchased from an appropriate and reputable supplier	√	√			
Identifying the need for additional password-protected email accounts for management, educators, staff and others at the service, and providing these as appropriate	√	√			
Identifying the training needs of educators and staff in relation to ICT, and providing recommendations for the inclusion of training in ICT in professional development activities	√	√			

Ensuring regular backup of critical data and information at the service *(refer to Attachment 1)*	√	√	√		
Ensuring secure storage of all information at the service, including backup files *(refer to Privacy and Confidentiality Policy)*	√	√	√		
Adhering to the requirements of the *Privacy and Confidentiality Policy* in relation to accessing information on the service's computer/s, including emails	√	√	√		
Ensuring that reputable anti-virus and firewall software *(refer to Definitions)* are installed on service computers, and that software is kept up to date	√	√			
Developing procedures to minimise unauthorised access, use and disclosure of information and data, which may include limiting access and passwords *(refer to Definitions)*	√	√			
Ensuring that the service's liability in the event of security breaches, or unauthorised access, use and disclosure of information and data is limited by developing and publishing appropriate disclaimers *(refer to Definitions)*	√	√			
Developing procedures to ensure data and information (e.g. passwords) are kept secure, and only disclosed to individuals where necessary e.g. to new educators, staff or committee of management	√	√			
Being aware of the requirements and complying with this policy	√	√	√	√	√
Appropriate use of endpoint data storage devices *(refer to Definitions)* by ICT users at the service	√	√	√		√
Ensuring that all material stored on endpoint data storage devices is also stored on a backup drive, and that both device and drive are kept in a secure location	√	√	√		√
Ensuring that written permission is provided by parents/guardians for authorised access to the service's computer systems and internet by persons under 18 years of age (e.g. a student on placement at the service) *(refer to Attachment 5).*	√	√			√
Providing authorisation to educators and staff to be social media representatives for St Francis of Assisi OSHC *(refer to Attachment 3)*	√	√			
Complying with all relevant legislation and service policies, protocols and procedures, including those outlined in *Attachments 1*	√	√	√	√	√
Reading and understanding what constitutes inappropriate use of ICT *(refer to Attachment 2)*	√	√	√		√
Completing the authorised user agreement form *(refer to Attachment 4)*	√	√	√		√
Maintaining the security of ICT facilities belonging to St Francis of Assisi OSHC and keeping allocated passwords secure, including not sharing passwords and logging off after using a computer	√	√	√		√
Accessing accounts, data or files on the service's computers only where authorisation has been provided		√	√		√

Co-operating with other users of the service's ICT to ensure fair and equitable access to resources	√	√	√		√
Obtaining approval from the approved provider before purchasing licensed computer software and hardware		√	√		
Ensuring no illegal material is transmitted at any time via any ICT medium *(refer to Attachment 2)*	**√**	√	√	√	√
Using the service's email, messaging and social media *(refer to Definitions)* facilities for service-related and lawful activities only *(refer to Attachment 2)*	√	√	√	√	√
Using endpoint data storage devices *(refer to Definitions)* supplied by the service for service-related business only, and ensuring that this information is protected from unauthorised access and use		√	√		√
Notifying the approved provider of any damage, faults or loss of endpoint data storage devices		**√**	**√**		**√**
Signing an acknowledgement form upon receipt of a USB or portable storage device (including a laptop) *(refer to Attachment 4)*		√	√		√
Restricting the use of personal mobile phones to rostered breaks, and only used in areas outside of spaces being utilised for education and care of children	√	√	√		√
Responding only to emergency phone calls when responsible for supervising children to ensure adequate supervision of children at all times *(refer to Supervision of Children Policy)*	√	√	√		√
Ensuring electronic files containing information about children and families are kept secure at all times *(refer to Privacy and Confidentiality Policy)*	**√**	**√**	**√**		**√**
Responding to a privacy breach in accordance with *Privacy and Confidentiality policy.*	**√**	√			
Complying with the appropriate use of social media *(refer to Definitions)* platforms *(refer to Attachment 3)*	√	√	√		√
Complying with this policy at all times to protect the privacy, confidentiality and interests of St Francis of Assisi OSHC employees, children and families	**√**	**√**	**√**		**√**
BOLD tick √ indicates legislation requirement					

PROCEDURES

Refer to *Attachment 1* for the following procedures

- Email usage
- Digital storage of personal and health information
- Data back up
- Password management

BACKGROUND AND LEGISLATION

BACKGROUND

The ICT environment is continually changing. Early childhood Services and School Age Services A now have access to a wide variety of technologies via fixed, wireless and mobile devices. While ICT is a cost-effective, timely and efficient tool for research, communication and management of a service, there are also legal responsibilities in relation to information privacy, security and the protection of employees, families and children.

State and federal laws, including those governing information privacy, copyright, occupational health and safety, anti-discrimination and sexual harassment, apply to the use of ICT *(refer to Legislation and standards).* Illegal and inappropriate use of ICT resources includes pornography, fraud, defamation, breach of copyright, unlawful discrimination or vilification, harassment (including sexual harassment, stalking and privacy violations) and illegal activity, including illegal peer-to-peer file sharing.

LEGISLATION AND STANDARDS

Relevant legislation and standards include but are not limited to:

- Broadcasting Services Act 1992 (Cth)
- Charter of Human Rights and Responsibilities Act 2006 (Vic)
- Crimes Act 1958 (Vic)
- Classification (Publications, Films and Computer Games) Act 1995
- Commonwealth Classification (Publication, Films and Computer Games) Act 1995
- Competition and Consumer Act 2010 (Cth)
- Copyright Act 1968 (Cth)
- Copyright Amendment Act 2006 (Cth)
- Cybercrime Act 2001 (Cth)
- Education and Care Services National Law Act 2010
- Education and Care Services National Regulations 2011
- Equal Opportunity Act 2010 (Vic)
- Freedom of Information Act 1982
- Health Records Act 2001 (Vic)
- Information Privacy Act 2000 (Vic)
- National Quality Standard, Quality Area 7: Governance and Leadership
- Occupational Health and Safety Act 2004 (Vic)
- Privacy Act 1988 (Cth)
- Privacy and Data Protection Act 2014 (Vic)
- Protected Disclosure Act 2012 (Vic)
- Public Records Act 1973 (Vic)
- Sex Discrimination Act 1984 (Cth)
- Spam Act 2003 (Cth)
- Trade Marks Act 1995 (Cth)

The most current amendments to listed legislation can be found at:

- Victorian Legislation – Victorian Law Today: www.legislation.vic.gov.au
- Commonwealth Legislation – Federal Register of Legislation: www.legislation.gov.au

DEFINITIONS

The terms defined in this section relate specifically to this policy. For regularly used terms e.g. Approved Provider, Nominated Supervisor, Notifiable Complaints, Serious Incidents, Duty of Care, etc. refer to the Definitions file of the PolicyWorks catalogue.

Anti-spyware: Software designed to remove spyware: a type of malware *(refer to Definitions),* that collects information about users without their knowledge.

Chain email: An email instructing recipients to send out multiple copies of the same email so that circulation increases exponentially.

Computer virus: Malicious software programs, a form of malware *(refer to Definitions)*, that can spread from one computer to another through the sharing of infected files, and that may harm a computer system's data or performance.

Cyber safety: The safe and responsible use of technology including use of the internet, electronic media and social media in order to ensure information security and personal safety. There are three main areas of risk to safety:

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interactions with other users (including bullying)
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Defamation: To injure or harm another person's reputation without good reason or justification. Defamation is often in the form of slander or libel.

Disclaimer: Statement(s) that seeks to exclude or limit liability and is usually related to issues such as copyright, accuracy and privacy.

Electronic communications: Email, instant messaging, communication through social media and any other material or communication sent electronically.

Encryption: The process of systematically encoding data before transmission so that an unauthorised party cannot decipher it. There are different levels of encryption available.

Endpoint data storage devices: Devices capable of storing information/data. New devices are continually being developed, and current devices include:

- laptops
- USB sticks, external or removable hard drives, thumb drives, pen drives and flash drives
- iPods or other similar devices
- cameras with USB drive connection
- iPhones/smartphones
- PCI/PC Card/PCMCIA storage cards
- PDAs (Personal Digital Assistants)
- other data-storage devices (CD-ROM and DVD).

Firewall: The primary method of keeping a computer/network secure. A firewall controls (by permitting or restricting) traffic into and out of a computer/network and, as a result, can protect these from damage by unauthorised users.

Flash drive: A small data-storage device that uses flash memory, and has a built-in USB connection. Flash drives have many names, including jump drives, thumb drives, pen drives and USB keychain drives.

Information sharing platforms: Describes the exchange of data between various organisations, people and technologies This can include but no limited to Dropbox, Google Drive, Sharepoint, Skype for Business, One Drive

Integrity: (In relation to this policy) refers to the accuracy of data. Loss of data integrity may be either gross and evident (e.g. a computer disk failing) or subtle (e.g. the alteration of information in an electronic file).

Malware: Short for 'malicious software'. Malware is intended to damage or disable computers or computer systems.

PDAs (Personal Digital Assistants): A handheld computer for managing contacts, appointments and tasks. PDAs typically include a name and address database, calendar, to-do list and note taker.

Wireless PDAs may also offer email and web browsing, and data can be synchronised between a PDA and a desktop computer via a USB or wireless connection.

Portable storage device (PSD) *or* **removable storage device (RSD):** Small, lightweight, portable easy-to-use device that is capable of storing and transferring large volumes of data. These devices are either exclusively used for data storage (for example, USB keys) or are capable of multiple other functions (such as iPods and PDAs).

Security: (In relation to this policy) refers to the protection of data against unauthorised access, ensuring confidentiality of information, integrity of data and the appropriate use of computer systems and other resources.

Social Media: A computer-based technology that facilitates the sharing of ideas, thoughts, information and photos through the building of virtual networks and communities**.** Examples can include but not limited to, Facebook, YouTube, WhatsApp, Facebook Messenger, TikTok and Instagram

Spam: Unsolicited and unwanted emails or other electronic communication.

USB interface: Universal Serial Bus (USB) is a widely used interface for attaching devices to a host computer. PCs and laptops have multiple USB ports that enable many devices to be connected without rebooting the computer or turning off the USB device.

USB key: Also known as sticks, drives, memory keys and flash drives, a USB key is a device that plugs into the computer's USB port and is small enough to hook onto a key ring. A USB key allows data to be easily downloaded and transported/transferred.

Virus: A program or programming code that multiplies by being copied to another program, computer or document. Viruses can be sent in attachments to an email or file, or be present on a disk or CD. While some viruses are benign or playful in intent, others can be quite harmful: erasing data or requiring the reformatting of hard drives.

SOURCES AND RELATED POLICIES

SOURCES

- Acceptable Use Policy, DET Information, Communications and Technology (ICT) Resources: https://www.education.vic.gov.au/school/teachers/management/infrastructure/Pages/acceptableuse.aspx
- IT for Kindergartens: www.kindergarten.vic.gov.au

RELATED POLICIES

- Code of Conduct
- Complaints and Grievances
- Enrolment and Orientation
- Governance and Management of the Service
- Occupational Health and Safety
- Privacy and Confidentiality
- Staffing

EVALUATION

In order to assess whether the values and purposes of the policy have been achieved, the Approved Provider will:

- regularly seek feedback from everyone affected by the policy regarding its effectiveness
- monitor the implementation, compliance, complaints and incidents in relation to this policy
- keep the policy up to date with current legislation, research, policy and best practice
- revise the policy and procedures as part of the service's policy review cycle, or as required
- notifying all stakeholders affected by this policy at least 14 days before making any significant changes to this policy or its procedures, unless a lesser period is necessary due to risk

ATTACHMENTS

- Attachment 1: Procedures for use of ICT at the service
- Attachment 2: Unacceptable/inappropriate use of ICT facilities
- Attachment 3: Social Media Guidelines
- Attachment 4: Authorised user agreement
- Attachment 5: Parent/guardian authorisation for under-age access to the St Francis of Assisi OSHC ICT facilities:

ATTACHMENT 1. PROCEDURES FOR USE OF ICT AT THE SERVICE

Email usage

- Content of emails and email addresses must always be checked before sending.
- When sending emails to multiple recipients, care should be taken to avoid the inappropriate disclosure of email addresses to a whole group of recipients; blind copying (BCC) should be used where appropriate.
- Always include a subject description in the subject line.
- Create an email signature that identifies employee name, title, service name, service phone number and address
- Always include a disclaimer *(refer to Definitions)* which is common to all users, on emails to limit liability.
- Be cautious about opening files or launching programs that have been received as an attachment via email from the email itself. Instead, save an attachment to disk and scan with anti-virus software before opening, and keep an eye out for unusual filenames.
- Never open emails if unsure of the sender.
- Check email accounts on a regular basis and forward relevant emails to the approved provider or appropriate committee members/staff.
- Remove correspondence that is no longer required from the computer quarterly.
- Respond to emails as soon as is practicable.
- Never send unauthorised marketing content or solicitation emails
- Be suspicious of clickbait titles.

Digital storage of personal and health information

- Digital records containing personal, sensitive and/or health information, or photographs of children must be password protected and stored securely so that privacy and confidentiality is maintained. This information must not be removed from the service without authorisation, as security of the information could be at risk *(refer to Privacy and Confidentiality Policy).*
- Digital records containing personal, sensitive and/or health information, or photographs of children may need to be removed from the service from time-to-time for various reasons, including for:
    - excursions and service events *(refer to Excursions and Service Events Policy)*
    - offsite storage, where there is not enough space at the service premises to store the records.

  In such circumstances, services must ensure that the information is transported, handled and stored securely so that privacy and confidentiality is maintained at all times.
- ICT users are not to view or interfere with other users' files or directories, knowingly obtain unauthorised access to information or damage, delete, insert or otherwise alter data without permission.
- Ensure all material stored on an endpoint data storage device is also stored on a backup drive, and that both device and drive are kept in a secure location.

Backing up data

Data backup is the process of creating accessible data copies for use in the event of breach or loss.

- Develop a written backup plan that identifies:
    - What's being backed up
    - Where it's being backed up
    - How often backups will occur
    - Who's in charge of performing backups
    - Who's in charge of monitoring the success of these backups
    - How will backup drives be stored securely

Services can choose to either between onsite or remote backup:

- Onsite Backup
    - copy data to a second hard drive, either manually or at specified intervals.
- Remote Backup- cloud based backup server
    - install the software on every computer containing data that needs to be backed up,
    - set up a backup schedule, and
    - identify the files and folders to be copied.

Password management

The effective management of passwords is the first line of defence in the electronic security of an organisation. Every ICT facility should have a password strategy in place as part of the overall security strategy. The technical considerations and principals outlined below are intended to be used as a guide for developing a password procedure.

Technical considerations include:

- a strong password should:
  - Be at least 8 characters in length
  - Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)
  - Have at least one numerical character (e.g. 0-9)
  - Have at least one special character (e.g. ~!@#$%^&*()_-+=)
- always verify a user's identity before resetting a password
- change passwords when an employer leaves the service
- password rotation; changed every 90 days or less
- do not use automatic logon functionality
- use of account lockouts for incorrect passwords, with a limit of 5 or fewer bad attempts.

Users should always follow these principles:

- do not share passwords with anyone. If there is an issue that requires you to do so, remember to change the password immediately after the issue has been resolved.
- never use the same password for work accounts as the one you have for personal use (banking, etc.).
- do not write down passwords or include them in an email.
- do not store passwords electronically unless they are encrypted.
- never use the "remember password" feature on any systems; this option should be disabled
- Do not use the same password for multiple administrator accounts.

Working from home

When an approved provider, nominated supervisor, educators or staff members are working from home they must:

- complete the authorised user agreement form *(refer to Attachment 4)*
- ensure security and confidentiality of work space, keeping private, sensitive, heath information, planning, educational programs and children's records confidential and secure at all times
- keep allocated passwords secure, including not sharing passwords and logging off after using a computer
- adhere to the *Privacy and Confidently Policy*
- report breaches to privacy or loss of private, sensitive, and heath information to nominated superiors as soon as practically possible.

ATTACHMENT 2. UNACCEPTABLE/INAPPROPRIATE USE OF ICT FACILITIES

Users of the ICT facilities (and in particular, the internet, email and social media) provided by St Francis of Assisi OSHC must not:

- create or exchange messages that are offensive, harassing, obscene or threatening
- create, copy, transmit or retransmit chain emails *(refer to Definitions)*, spam *(refer to Definitions)* or other unauthorised mass communication
- use the ICT facilities as a platform to gain unauthorised access to other systems
- carry out activities that are illegal, inappropriate or offensive to fellow employees or the public. Such activities include, but are not limited to, hate speech or material that ridicules/discriminates against others on the basis of race, nationality, creed, religion, ability/disability, gender or sexual orientation
- use the ICT facilities to access, download, create, store or distribute illegal, offensive, obscene or objectionable material (including pornography and sexually explicit material). It will not be a defence to claim that the recipient was a consenting adult
- use the ICT facilities to make any personal communication that could suggest that such communication was made in that person's official capacity as an employee or volunteer of St Francis of Assisi OSHC
- conduct any outside business or engage in activities related to employment with another organisation
- play games
- use the facilities to assist any election campaign or lobby any government organisation
- exchange any confidential or sensitive information held by St Francis of Assisi OSHC unless authorised as part of their duties
- publish the service's email address on a 'private' business card
- harass, slander, intimidate, embarrass, defame, vilify, seek to offend or make threats against another person or group of people
- breach copyright laws through making copies of, or transmitting, material or commercial software.

Breaches of this policy

- Individuals who use ICT at the service for unlawful purposes may be liable to criminal or civil legal action. This could result in serious consequences, such as a fine, damages and/or costs being awarded against the individual, or imprisonment. The Approved Provider will not defend or support any individual using the service's ICT facilities for an unlawful purpose.
- The service may block access to internet sites where inappropriate use is identified.
- Employees who fail to adhere to this policy may be liable to counselling, disciplinary action or dismissal.
- Management, educators, staff, volunteers and students who fail to adhere to this policy may have their access to the service's ICT facilities restricted/denied.

Category 1: illegal — criminal use of material

This category includes but is not limited to:

- child abuse material offences relating to child pornography covered by the Crimes Act 1958 (Vic). 'Child abuse material' is defined in section 51A of the Crimes Act 1958 (Vic)
- objectionable material — offences relating to the exhibition, sale and other illegal acts relating to 'objectionable films' and 'objectionable publications' covered by the Classification (Publications, Films and Computer Games) (Enforcement) Act 1995 (Vic). Such material has or would attract a classification of X18+ (restricted) or RC (refused classification) under the Guidelines for Classification of Films 2012, Guidelines for the Classification of Computer Games 2012 or National Classification Code scheduled to the Classification (Publications, Films and Computer Games) Act 1995 (Cth)
- reckless or deliberate copyright infringement
- any other material or activity that involves or is in furtherance of a breach of criminal law

Category 2: extreme — non-criminal use of material

This category includes non-criminal use of material that has or may attract a classification of RC or X18+ under the Guidelines for Classification of Films 2012, Guidelines for the Classification of Computer Games 2012 or National Classification Code scheduled to the Classification (Publications, Films and Computer Games) Act 1995 (Cth).

This includes any material that:

- depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that the material should not be classified
- describes or depicts in a way that is likely to cause offence to a reasonable adult or a person who is, or appears to be, a child under 18 (whether or not the person is engaged in sexual activity or not)
- promotes, incites or instructs in matters of crime or violence
- includes sexually explicit material that contains real depictions of actual sexual intercourse and other sexual activity between consenting adults

Category 3: critical — offensive material

This category includes other types of restricted or offensive material, covering any material that:

- has or may attract a classification of R18+ under the Guidelines for Classification of Films 2012, Guidelines for the Classification of Computer Games 2012 or National Classification Code scheduled to the Classification (Publications, Films and Computer Games) Act 1995 (Cth). Material may contain sex scenes and drug use that are high in impact
- includes sexualised nudity
- involves racial or religious vilification
- is unlawfully discriminatory
- is defamatory
- involves sexual harassment or bullying

Category 4: serious

- This category includes any use which is offensive or otherwise improper.
- The categories do not cover all possible breaches of this policy. Matters not covered by the above categories will be dealt with on an individual basis and on the relevant facts.

ATTACHMENT 3. SOCIAL MEDIA AND INFORMATION SHARING PLATFORM GUIDELINES

The below directives are essential to the safety and wellbeing of staff, children and their families, and to ensure that St Francis of Assisi OSHC operates in a professional and appropriate manner when using social media and/or information sharing platforms.

Staff must exercise extreme caution using ICT facilities when accessing social media and/or information sharing platforms, whether in the workplace or relating to external events or functions involving St Francis of Assisi OSHC.

It is a breach of confidentiality and privacy to make posts or comments about children, families, staff or management from St Francis of Assisi OSHC on social media sites without consent or authorisation. It is also an offence under current legislation, to record or use a visual image of a child, including transmitting the image on the internet, without the written consent of the child's parent.

St Francis of Assisi OSHC specifically requires that, unless you have the express permission, you:

- Do not video or photograph anyone, or post photos or personal details of other St Francis of Assisi OSHC staff, children or families;
- Do not post photos or videos of St Francis of Assisi OSHC staff, children or families on your personal Facebook page, or otherwise share photos or videos of staff, children or families through social media;
- Do not create a St Francis of Assisi OSHC branded Facebook page, or other pages or content on social media that represents St Francis of Assisi OSHC, it's staff, children or families without authorisation from the approved provider;
- Do not post anything that could embarrass or damage the reputation of St Francis of Assisi OSHC, colleagues, children or families.

Staff must not:

- post or respond to material that is, or might be construed as offensive, obscene, fraudulent, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, infringes copyright, constitutes a contempt of court, breaches a Court suppression order, or is otherwise unlawful or inaccurate;
- make any comment or post any material that might otherwise cause damage to St Francis of Assisi OSHC reputation or bring it into disrepute;
- imply that they are authorised to speak as a representative of St Francis of Assisi OSHC, or give the impression that the views expressed are those of St Francis of Assisi OSHC , unless authorised to do so
- use a St Francis of Assisi OSHC email address or any St Francis of Assisi OSHC logos or insignia that may give the impression of official support or endorsement of personal comments;
- use the identity or likeness of another employee, contractor or other member of St Francis of Assisi OSHC;
- use or disclose any confidential information or personal information obtained in the capacity as an employee/contractor of St Francis of Assisi OSHC; or
- access and/or post on personal social media during paid workhours.

Personal use of social media

St Francis of Assisi OSHC recognises that staff may choose to use social media in their personal capacity. This policy is not intended to discourage nor unduly limit staff using social media for personal expression or other online activities in their personal life. Staff should be aware of and understand the potential risks and damage to St Francis of Assisi OSHC that can occur through their use of social media, even if their activity takes place outside working hours or on devices not owned by St Francis of Assisi OSHC.

If an individual can be identified as an employee of St Francis of Assisi OSHC on social media, that employee must:

- only disclose and discuss publicly available information;
- ensure that all content published is accurate and not misleading and, complies with all relevant policies of St Francis of Assisi OSHC
- expressly state on all postings (identifying them as an employee of St Francis of Assisi OSHC) the stated views are their own and are not those of St Francis of Assisi OSHC;
- be polite and respectful to all people they interact with;
- adhere to the Terms of Use of the relevant social media platform/website, as well as copyright,
- abide by privacy, defamation, contempt of Court, discrimination, harassment and other applicable laws;

- ensure that abusive, harassing, threatening or defaming postings which are in breach of St Francis of Assisi OSHC policies may result in disciplinary action being taken, even if such comments are made using private social networks outside of working hours.
- notify the approved provider or person with management or control if they become aware of unacceptable use of social media as described above.

Consequences of unacceptable use of social media

- St Francis of Assisi OSHC will review any alleged breach of this policy on an individual basis. If the alleged breach is of a serious nature, the person shall be given an opportunity to be heard in relation to the alleged breach.
- If the alleged breach is clearly established, the breach may be treated as grounds for dismissal. In all other cases, the person may be subject to disciplinary action in accordance with St Francis of Assisi OSHC *Code of Conduct Policy*.
- St Francis of Assisi OSHC may request that any information contained on any social media platform that is in breach of this policy be deleted.
- St Francis of Assisi OSHC may restrict an employee's access to social media on [St Francis of Assisi OSHC ICT facilities or if they are found to have breached this policy or while St Francis of Assisi OSHC investigates whether they have breached this policy.

ATTACHMENT 4. AUTHORISED USER AGREEMENT

Portable storage device (PSD) (including laptops)

I, _____ ,

- acknowledge that I have received a PSD belonging to St Francis of Assisi OSHC
- will ensure that the PSD:
    - is used for work-related purposes only
    - is password-protected at all times
    - will not be loaned to unauthorised persons
    - will be returned to St Francis of Assisi OSHC on cessation of employment
- will notify the Co-ordinator as soon as is practicable if the PSD is damaged, faulty or lost
- have read the St Francis of Assisi OSHC Information and Communication (ICT) Technology Policy and agree to abide by the procedures outlined within.

_____ _____

Signature (authorised user) Position

_____

Date

_____ _____

Authorised by Position

_____

Date

ATTACHMENT 5. PARENT/GUARDIAN AUTHORISATION FOR UNDER-AGE ACCESS TO THE ST FRANCIS OF ASSISI OSHC ICT FACILITIES

Student's name: _____

Date of placement:_____

I, _____ , am a parent/guardian of

_____

I have read the St Francis of Assisi OSHC *Information and Communication Technology (ICT) Policy* and agree to the conditions of use of the service's ICT facilities for the above-named student.

I also understand that St Francis of Assisi OSHC provides no censorship of access to ICT facilities.

_____ _____

Signature (student) Date

_____ _____

Signature (parent/guardian) Date