COMPUTER AND INFORMATION TECHNOLOGY POLICY

NQS

Element 4.2: Management, educators and staff are collaborative, respectful and ethical,
Element 4.2.2: Professional standards guide practice, interactions and relationships
Element 7.1: Governance supports the operation of a quality service
Element 7.1.2: Systems are in place to manage risk and enable the effective management and operation of a quality service
Early Childhood and Care Services National Regulations

PURPOSE

The purpose of this policy is to outline the acceptable use of computer equipment at FROEBEL Australia Limited ("FROEBEL"). It also provides procedures for selection and use of IT within FROEBEL. These rules are in place to protect the employee and FROEBEL. Inappropriate use exposes FROEBEL to risks including virus attacks, compromise of network systems and services, and legal issues.

SCOPE

This policy applies to all equipment, to the use of information, electronic, media, computing devices, personal smart phones, smart watches and network resources to conduct FROEBEL business or interact with internal networks and business systems, whether owned or leased by FROEBEL, the employee, or a third party. All employees at FROEBEL are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with FROEBEL policies and standards, and local laws and regulation.

POLICY

3.1 General Use and Ownership

The use of FROEBEL electronic systems, including laptops/computers/tablets, the server, copier, data projectors and all forms of Internet/Intranet access, is for FROEBEL business and for authorised purposes only. Brief and occasional personal use of the electronic systems or the Internet is acceptable as long as it is not excessive or inappropriate, occurs during personal time (lunch or other breaks), and does not result in expenses or harm to FROEBEL or otherwise violate this policy. Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job responsibilities.

3.1.1 Employees agree to the following actions regarding Company Laptops:

- Employees are discouraged from installing personal software on a company laptop.
- Employee will not use company laptop for excessive personal use such as personal emails, IMs, web browsing, etc.
- Employee will report Loss or Theft of company laptop immediately.

- Employee will take all reasonable measures to ensure the physical and digital security of the laptop
- Employee will not download and/or save any Company data and content to third party or personal devices (e.g. personal home computer, USB drives, etc.)
- In the event of termination, all company property, including Company Laptops and all stored proprietary information and your work, must be returned to the employer.

3.1.2 Working off-site is accepted. The following controls must be applied:

- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling and never be left unattended.
- It is a requirement for staff to complete a sign out and in register when borrowing multi-media equipment, such as projectors and cameras.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used (user password).

3.1.3 FROEBEL proprietary information stored on electronic and computing devices, whether owned or leased by FROEBEL, the employee or a third party, remains the sole property of FROEBEL.

3.1.4 You have a responsibility to promptly report the theft, loss or unauthorised disclosure of FROEBEL proprietary information.

3.1.5 You may access, use or share FROEBEL proprietary information only to the extent it is authorised and necessary to fulfil your assigned job duties.

3.1.6 Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

3.1.7 For security and network maintenance purposes, authorised individuals within FROEBEL and duly contracted third party IT systems managers may monitor equipment, systems and network traffic at any time. FROEBEL also reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

3.2 Security and Proprietary Information

3.2.1 Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

3.2.2 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. If you are working off-site, you must lock the screen or log off when the device is unattended.

3.2.3 Postings by employees from a FROEBEL email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of FROEBEL, unless posting is in the course of business duties.

3.2.4 Employees must use caution when opening e-mail attachments received from unknown senders, which may contain malware.

3.2.5 Employees must ensure that antivirus software is installed and maintained on laptops/computers as required by FROEBEL.

3.2.6 Employees must ensure that backup software is installed and maintained on laptops/computers as required by FROEBEL.

3.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities. Under no circumstances is an employee of FROEBEL authorised to engage in any activity that is illegal under local, state, federal or international law while utilising FROEBEL-owned resources.

The lists below are by no means exhaustive, they provide a framework for activities which fall into the category of Unacceptable Use.

3.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by FROEBEL.

2. Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books, booklets or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which FROEBEL or the end user does not have an active license is strictly prohibited.

3. Accessing data, a server or an account for any purpose other than conducting FROEBEL business, even if you have authorised access, is prohibited.

4. Exporting software, technical information, encryption software or technology, on your personal device or in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

6. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties.

7. Providing information about, or lists of, FROEBEL employees and/or customers (including children) to parties outside FROEBEL.

3.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realise they represent FROEBEL. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". The following activities are not permitted:

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Use of unsolicited email originating from within FROEBEL's networks of other Internet/Intranet service providers on behalf of, or to advertise, any service hosted by FROEBEL or connected via FROEBEL's network.

4. Disclosing email recipients in non-individual group emails (recipients' email addresses must always be blind copied).

3.3.3 Blogging and Social Media

1. Blogging by employees, whether using FROEBEL's property and systems or personal computer systems, is also subject to the terms and restrictions set in the Social Media Policy.

Limited and occasional use of FROEBEL's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate FROEBEL's policy, is not detrimental to FROEBEL's best interests, and does not interfere with an employee's regular work duties. Blogging from FROEBEL's systems is also subject to manager approval and monitoring.

2. FROEBEL's Privacy and Confidentiality policy also applies to blogging. As such, Employees are prohibited from revealing any FROEBEL confidential or proprietary information, trade secrets or any other material covered by FROEBEL's Confidential Information policy when engaged in blogging.

3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of FROEBEL and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments.

4. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, FROEBEL's trademarks, logos and any other FROEBEL intellectual property may also not be used in connection with any blogging activity.

3.3.4 Smart phones, smart watches and personal devices

1. The use of personal devices, smart phones and watches for calls, messaging or other personal activity is restricted to use in rostered break times

2. Personal phones or devices must not be used to take photos of children within the service or when out on excursions.

3. A personal device may be used to access music (such as Spotify) to support the educational program, the use of a personal device for such circumstances is at the Managers/ Centre Directors discretion.

4. A personal device may be used by nominated fire wardens in case of emergencies as per the Emergency Management Plans at each service.

5. Improper use of personal devices whilst on rostered time may result in disciplinary action as outlined in the Code of Conduct and Ethics Policy.

User compliance

I understand and will abide by this Computer and Information Technology Policy. I further understand that should I commit any breach of this policy; my access privileges may be revoked, disciplinary action and/or appropriate legal action may be taken.

Full Name: _____

Signature:_____Date:_____

ASSOCIATED POLICIES

- Code of Conduct and Ethics
- Emergency Management Plans
- Professional Boundaries and Protective Practices Policy
- Privacy and Confidentiality
- Social Media Policy

POLICY REVIEW

- FROEBEL will review this policy every 12 months.
- The Approved Provider and Nominated Supervisor ensure that all educators always maintain and implement this policy and its procedures.

- **Last review**: 28.09.2022
- **Next review**: 28.09.2023