IT Security Policy

Information technology services play a vital role in the functioning of our Centre. They are used to store private, conduct most financial transactions. Were the security of our IT systems to be compromised, there are a variety of serious potential consequences. Some of these relate to breaches of privacy (as discussed in the privacy policy), others relate to continuity of business operations or financial losses.
Therefore, the crèche must actively manage its IT systems to reduce the risk of security incidents, and reduce the consequences were an incident to occur.

The nominated supervisor will ensure:

- That a register of all software and cloud services used by crèche is maintained. A copy must be kept offline in a secure location.
- All software used within crèche must be licensed and kept up to date. Software that is no longer supported by a vendor should not be used.
- Private information is stored only on systems and services approved for use. If a staff member wants to use a new system that requires private information, it must be approved by the nominated supervisor?.
- The nominated supervisor should conduct a basic risk analysis before adopting a new IT system or service. The supervisor should consider:
    - The nature of the information shared with the service.
    - How the service makes use of that information.
    - The service's privacy and security policies.
    - Available information about their security and privacy track record, if any. Lack of any such track record should be a considered a risk.
    - The jurisdiction they operate in (services with an Australian presence and bound by Australian law represent a lower risk).
    - What the potential consequences of the information stored on the service being hacked are.
    - What the potential consequences of the service becoming unavailable are.
- Effective anti-malware software is installed on all applicable systems.
- Where possible, all staff are issued individual accounts to access IT system and services.
- IT administrative accounts are not used for regular work (this will mean that staff who perform IT administration may have two or more accounts).
- An up-to-date copy of all administrative account credentials is kept securely offline, sufficient to recover access to all systems.
- As far as is practical, staff members do not have access to systems and information not needed to do their jobs.
- Access to IT facilities is revoked as soon as is practical after the staff member or committee member no longer serves in a role requiring access.
- Where passwords are used to access accounts, strong, unique passwords are used. The use of password managers is recommended.
- Where practical, multi-factor authentication is used to access IT resources.
- All information stored by the crèche is backed up frequently and in a redundant manner. Off-site encrypted backups should be maintained.
- A disaster recovery plan to restore IT systems must be developed.
- Disaster recovery tests involving restoring the crèche's systems from backups must be conducted annually.
- All data stored on devices physically owned by the crèche must be deleted securely before disposing of the device.
- Staff should be trained on IT security policies and practices relevant to their use of IT. For instance, this might include phishing awareness training.
- An IT professional is engaged on an annual basis (or more frequently if required) to audit the security of the Crèche's IT systems, and recommend updates to this policy if required.

Staff and volunteers (including Committee members) will:

- Choose unique, strong passwords to access Centre IT systems.
- Not provide their account credentials to anyone else. IT support should never ask for it.
- Not share access to Centre IT systems with anyone else.
- Not use private IT systems for work.
- Report any signs of an attempted or actual IT security breach to the nominated supervisor as soon as possible.

Parents will:

- Not share access to the centre's IT systems (e.g. Xplor) with anyone.
- Report any suspected or actual IT security incidents to the Centre as soon as possible.

Source: Australian Children's Education & Care Quality Authority. (2014). Guide to the Education and Care Services National Law and the Education and Care Services National Regulations 2015, ECA Code of Ethics, Guide to the National Quality Standard, Work Health and Safety Act 2011, IT Consultant – One Call Computer Services.
Date Implemented: 01/10/2020
Review Completed: 29/03/2021
Schedule for Review: 29/03/2022
Authorised by COM: Nov 2020

National Quality Standard – NQS		
Quality Area 4: Staffing Arrangements		
4.2	Professionalism	Management, educators and staff are collaborative, respectful and ethical.
4.2.2	Professional Standards	Professional standards guide practice, interactions and relationships.
Quality Area 5: Relationships with Children		
5.1.2	Dignity and rights of the child	The dignity and rights of every child are maintained.
Quality Area 7: Leadership and Service Management		
7.1	Governance	Governance supports the operation of a quality service.
7.1.2	Management Systems	Systems are in place to manage risk and enable the effective management and operation of a quality service.
7.1.3	Roles and Responsibilities	Roles and responsibilities are clearly defined, and understood, and support effective decision-making and operation of the service.
7.2	Leadership	Effective leadership builds and promotes a positive organisational culture and professional learning community.
Education and Care Service National Regulations		
727	Confidentiality of records kept by approved provider	
181-184	Confidentiality and storage of records	