INFORMATION AND TECHNOLOGY POLICY

BEST PRACTICE – QUALITY AREA 7

PURPOSE

VALUES

This policy will provide guidelines to ensure that all users of information and communication technology (ICT) at Highvale Preschool or on behalf of Highvale Preschool:

- understand and follow procedures to ensure the safe and appropriate use of ICT at the service
- take responsibility to protect and maintain privacy in accordance with the service's policies
- 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

SCOPE

This policy applies to the Approved Provider, Nominated Supervisor, Service Supervisors, educators, other staff, students on placement and volunteers at Highvale Preschool. This policy does not apply to children. This policy applies to all aspects of the use of ICT

BACKGROUND AND LEGISLATION

The Victorian Government has funded the provision of ICT infrastructure and support to kindergartens since 2003. Highvale Preschool has now moved on to its own private provider in order to have a faster and better service

Relevant legislation and standards include but are not limited to:

- *Broadcasting Services Act 1992* (Vic), as amended 2007
- *Competition and Consumer Act 2010* (Cth)
- *Copyright Act 1968* (Cth)
- *Copyright Amendment Act 2006* (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*
- *National Quality Standard*, Quality Area 7: Leadership and Service Management
- Standard 7.3: Administrative systems enable the effective management of a quality service
- *Occupational Health and Safety Act 2004*
- *Privacy Act 1988* (Cth)
- *Public Records Act 1973* (Vic)

PROCEDURES

THE APPROVED PROVIDER IS RESPONSIBLE FOR:

- 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*)
- providing suitable ICT facilities to enable educators and staff to effectively manage and operate the service
- ensuring that procedures are in place for the regular backup of critical data and information at the service
- ensuring secure storage of all information at the service, including backup files (refer to *Privacy and Confidentiality Policy*)
- considering encryption (refer to *Definitions*) of data for extra security
- ensuring that reputable anti-virus and firewall software (refer to *Definitions*) are installed on service computers, and that software is kept up to date

- 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
- ensuring compliance with this policy by all users of the service's ICT facilities

THE NOMINATED SUPERVISOR, SERVICE SUPERVISORS AND OTHER EDUCATORS/STAFF ARE RESPONSIBLE FOR:

- complying with all relevant legislation and service policies, protocols and procedures, including those outlined in Attachments 1 and 2
- keeping allocated passwords secure, including not sharing passwords and logging off after using a computer
- obtaining approval from the Approved Provider before purchasing licensed computer software and hardware
- ensuring confidential information is transmitted with password protection or encryption, as required
- ensuring no illegal material is transmitted at any time via any ICT medium
- notifying the Approved Provider of any damage, faults or loss of devices
- ensuring electronic files containing information about children and families are kept secure at all times (refer to *Privacy and Confidentiality Policy*).

ALL PARENTS/GUARDIANS ARE RESPONSIBLE FOR:

- reading and understanding this *Information and Communication Technology (ICT) Policy*
- complying with all state and federal laws, the requirements of the *Education and Care Services National Regulations 2011*, and all service policies and procedures
- maintaining the privacy of any personal or health information provided to them about other individuals e.g. contact details.

VOLUNTEERS AND STUDENTS, WHILE AT THE SERVICE, ARE RESPONSIBLE FOR FOLLOWING THIS POLICY AND ITS PROCEDURE

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
- notify parents/guardians at least 14 days before making any changes to this policy or its

ATTACHMENTS:

- Attachment 1: Procedures for use of ICT at the service
- Attachment 2: Guiding principles for security of information systems

AUTHORISATION:

Adopted by Highvale Preschool Association Inc. 9th August, 2016 and will take effect from 24th August, 2016

REVIEW DATE: July 2019

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.
- 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.
- 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.

UNACCEPTABLE/INAPPROPRIATE USE OF ICT FACILITIES

Users of the ICT facilities (and in particular, the internet, email and social media) provided by Highvale Preschool 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 Highvale Preschool
- conduct any outside business or engage in activities related to employment with another organisation
- play games
- assist any election campaign or lobby any government organisation
- 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.

INFORMATION STORED ON COMPUTERS

- Computer records containing personal, sensitive and/or health information, or photographs of children must be 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*).
- Computer 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.

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.

ATTACHMENT 2

Guiding principles for security of information systems

- The Organisation for Economic Co-operation and Development's (OECD) guidelines encourage an awareness and understanding of security issues and the need for a culture of security.
- The OECD describes nine guiding principles that encourage awareness, education, and information sharing and training as effective strategies in maintaining security of information systems. The guiding principles are explained in the table below.

Awareness	Users should be aware of the need for security of information systems and networks and what they can do to enhance security.
Responsibility	All users are responsible for the security of information systems and networks.
Response	Users should act in a timely and cooperative manner to prevent, detect and respond to security issues.
Ethics	Users should respect the legitimate interest of others.
Democracy	The security of information systems and networks should be compatible with the essential values of a democratic society.
Risk assessment	Users should conduct risk assessments.
Security design and implementation	Users should incorporate security as an essential element of information systems and networks.
Security management	Users should adopt a comprehensive approach to security management.
Reassessment	Users should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, measures and procedures.

Sourced from Organisation for Economic Co-operation and Development's (OECD) (2002) *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.*