ONLINE MEETING PLATFORM POLICY

Best Practice – Quality Area 7

PURPOSE

This policy will provide guidelines to ensure that all users of Online Meeting platforms at Gum Nut Gully Preschool or on behalf of Gum Nut Gully Preschool:

- understand and follow procedures to ensure the safe and appropriate use of Online Meeting platforms at the Service.
- 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 the online meeting platform at the Service
- understand what constitutes illegal and inappropriate use of Online Meeting facilities and avoid such activities.

POLICY STATEMENT

1. VALUES

Gum Nut Gully Preschool is committed to:

- professional, ethical and responsible use of Online Meetings at the Service
- providing a safe workplace for management, educators, staff and others using the Service's Online Meeting facilities
- safeguarding the privacy and confidentiality of information received, transmitted or stored electronically
- ensuring that the use of the Service's Online Meeting 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.

2. SCOPE

This policy applies to the Approved Provider, Persons with Management and Control, Nominated Supervisor, Persons in Day to Day Charge, educators, staff, Committee of Management volunteers and children enrolled at Gum Nut Gully Preschool.

This policy applies to all aspects of the use of Online Meetings including:

- electronic discussion/news group
- social networking
- file transfers
- file storage (including the use of end point data storage devices – refer to *Definitions*)
- file sharing
- video conferencing
- streaming media
- instant messaging
- online discussion groups and chat facilities
- copying, saving or distributing files
- viewing material electronically
- printing material

- portable communication devices including mobile and cordless phones.

3. Background and legislation

Background

During the 2020 Covid-19 Pandemic and the resulting restrictions implemented by the Victorian Government, it was apparent that an Online Meeting platform was required in order for the Preschool to continue its regular Services.

The need for an online platform was created for:

- Committee of Management Meetings
- Staff Meetings
- Parent/Teacher Interviews
- Remote delivery of Educational learning experience.

The Online Meeting environment is continually changing. Early childhood Services now have access to a wide variety of technologies via fixed, wireless and mobile devices. While Online Meetings are a cost-effective, timely and efficient tool for delivering educational content remotely, 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 Online Meetings (refer to *Legislation and standards*). Illegal and inappropriate use of Online Meeting 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)
- *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)
- *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)*
- *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: http://www.legislation.vic.gov.au/
- Commonwealth Legislation – ComLaw: http://www.comlaw.gov.au/

4. Definitions

The terms defined in this section relate specifically to this policy. For commonly used terms e.g. Approved Provider, Nominated Supervisor, Regulatory Authority etc. refer to the *General Definitions* section of this manual.

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

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.

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.

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).

Spam: Unsolicited and unwanted emails or other electronic communication.

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.

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.

Vicnet: An organisation that provides a range of internet Services to libraries and community groups (including kindergartens, as part of a government-funded project), including broadband and dial-up internet and email access, website and domain hosting, and website design and development. Vicnet delivers information and communication technologies, and support Services to strengthen Victorian communities. For more information, visit: www.kindergarten.vic.gov.au

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.

5. 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

Service policies

- *Code of Conduct Policy*
- *Complaints and Grievances Policy*
- *Curriculum Development Policy*
- *Enrolment and Orientation Policy*
- *Information & Communication Technology Policy*
- *Governance and Management of the Service Policy*
- *Occupational Health and Safety Policy*
- *Privacy and Confidentiality Policy*
- *Staffing Policy*

Procedures

The Approved Provider or Persons with Management and Control is responsible for:

- ensuring that the use of the Service's Online Meetings 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 Online Meeting facilities to enable educators and staff to effectively manage and operate the Service & deliver their online educational program.

- authorising the access of educators, staff, volunteers and students to the Service's Online Meeting facilities, as appropriate
- providing clear procedures and protocols that outline the parameters for use of the Service's Online Meeting facilities (refer to Attachment 1 – Procedures for use of ICT at the Service)
- embedding a culture of awareness and understanding of security issues at the Service (refer to Attachment 2 – Guiding principles for security of information systems)
- ensuring that the Service's Online Meeting platform 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 Online Meetings, and providing recommendations for the inclusion of training in online meetings in professional development activities
- 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*)
- adhering to the requirements of the *Privacy and Confidentiality Policy* in relation to accessing information on the Service's computer/s, including emails
- 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
- developing procedures to minimise unauthorised access, use and disclosure of information and data, which may include limiting access and passwords, and encryption (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. Parents/carers, educators, staff or committee of management
- developing procedures to ensure that all educators, staff, volunteers and parents are aware of the requirements of this policy
- ensuring the appropriate use of endpoint data storage devices (refer to *Definitions*) by all ICT users at the Service
- ensuring compliance with this policy by all users of the Service's Online Meeting facilities
- ensuring that written permission is provided by parents/guardians for authorised access to the Online Meeting platform by persons under 18 years of age(refer to Attachment 3 – Parent/guardian authorisation for under-age access to the Gum Nut Gully Pre School online meeting facilities).

The Nominated Supervisor, Person with Day to Day Charge, educators, staff and other authorised users of the Service's Online Meeting facilities are responsible for:

- complying with all relevant legislation and Service policies, protocols and procedures, including those outlined in Attachments 1 and 2
- completing the authorised user agreement form (see Attachment 4)
- keeping allocated passwords secure, including not sharing passwords and logging off after online meetings.
- Sharing meeting links securely & not via public channels or social media & sharing with authorised persons only.
- Ensuring passwords are always required to access Online Meetings.
- Ensuring any recordings of online meetings are conducted by the educator only and of the educator only.
- maintaining the security of online meeting facilities belonging to Gum Nut Gully Pre School

- co-operating with other users of the Service's online meeting to ensure fair and equitable access to resources
- obtaining approval from the Approved Provider before purchasing licensed Online Meeting computer software.
- ensuring confidential information is transmitted with password protection or encryption, as required
- ensuring no illegal material is transmitted at any time via any online meeting platform
- using the Service's online meeting, messaging and social media facilities for Service-related and lawful activities only.
- 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
- ensuring that 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
- 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.

Parents/guardians are responsible for:

- reading and understanding this *Online Meeting 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
- Ensuring that an adult is present at all times during an online meeting the child is attending.
- Ensuring the child is accessing an online meeting in a shared space.
- Ensuring the child is fully clothed at all times.
- Ensuring that only the child enrolled in the Service accesses the online meeting.
- Ensuring no Gum Nut Gully online meetings are recorded.

Volunteers and students, while at the Service, are responsible for following this policy and its procedures.

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 procedures.

Attachments

- Attachment 1: Procedures for use of Online Meetings at the Service
- Attachment 2: Guiding principles for security of information systems
- Attachment 3: Parent/guardian authorisation for under-age access to the Gum Nut Gully Pre School Online Meeting facilities
- Attachment 4: Authorised COM Volunteer Member user agreement

Authorisation

This policy was adopted by the Approved Provider of Gum Nut Gully Pre School on

REVIEW DATE: AUGUST 2023

Attachment 1
Procedures for use of Online Meetings at the Service

Unacceptable/inappropriate use of Online meeting facilities

Users of the Online Meeting facilities provided by Gum Nut Gully Preschool must not:

- create or exchange messages that are offensive, harassing, obscene or threatening
- record or share copies of recordings of Online Meetings hosted by Gum Nut Gully Preschool
- use the Online Meeting 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 Gum Nut Gully 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
- exchange any confidential or sensitive information held by Gum Nut Gully Preschool 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 Online Meetings 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 Online Meeting facilities for an unlawful purpose.
- 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 Online Meeting facilities restricted/denied.

ATTACHMENT 2
Guiding principles for security of Online Meetings

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, 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.*

ATTACHMENT 3

Parent/guardian authorisation for under-age access to Gum Nut Gully Preschool's Online Meeting facilities

Child's name:

I, , am a parent/guardian of

I have read the Gum Nut Gully Preschool *Online Meeting Policy* and agree to the conditions of use of the Service's Online Meeting facilities for the above-named child.

Signature (parent/guardian) Date

ATTACHMENT 4
Committee Of Management Volunteer Member Online Meeting user agreement

I, ,

- have read the Gum Nut Gully Preschool *Online Meeting Policy* and agree to abide by the procedures outlined within.
- will not record, invite or share meetings with unauthorised parties.

Signature (authorised user) Position

Date

Authorised by Position

Date