Information Technology, Internet, Email and Social Media Procedure

Policy

The Information Technology (IT), Internet, Email and Social Media Procedure falls under the Governance and Management of Service Policy.

Hawthorn Early Years (the Service) will ensure systems are in place to manage risk and enable the effective management and operation of a quality service. Roles and responsibilities will be clearly defined and understood and effective leadership used to build and promote a positive organisational culture and a professional learning community.

Background

The IT environment is continually changing. Early childhood services now have access to a wide variety of technologies via fixed, wireless and mobile devices. While IT 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.

Application of Procedure

This procedure applies to all employees, volunteers, students, the Board, families, children and others attending the activities and programs of HEY. This procedure applies to all aspects of Information Communication Technology (ICT) including (but not limited to):

- Internet usage
- Electronic mail (email), bulletins and notice boards
- Electronic discussions/news groups/information
- Weblogs (blogs) (e.g. Tumblr)
- Social networking (e.g. Twitter, Facebook, and LinkedIn)
- File transfer (downloading and uploading files)
- File storage (including the use of end point data storage devices)
- Video conferencing
- Streaming media
- Instant messaging
- Online discussion groups and chat facilities
- Subscription to list servers, mailing lists or other like services
- Printing material
- Image sharing sites (e.g. Instagram, snapchat)
- Audio & visual recording devices (e.g. camera, iPhone, iPad)
- Projecting devices (e.g. audio speakers, projector)

While the use of digital and social mediums can be beneficial, especially when sharing learning and information within the service, and externally to the service community, it is important that all stakeholders follow this procedure to ensure children, families', and educators' identity and integrity is respected, and that high levels of professionalism are maintained and promoted.

Key Definitions:

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, iPads or other similar devices
- cameras with USB drive connection
- smartphones
- PCI/PC Card/PCMCIA storage cards
- PDAs (Personal Digital Assistants)
- other data-storage devices (CD-ROM, DVD and Cloud).

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.

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

Spam: Unsolicited and unwanted emails or other electronic communications.

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

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: Includes the following platforms – social networking sites such as Facebook and LinkedIn, blogs and twitter, personal websites, online forums, discussion boards and any other website that allows companies and individuals to post comments on the web.

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.

Hawthorn Early Years is committed to:

The professional, ethical and responsible use of IT at the Service to:

- Provide a safe workplace for all employees, children and others using the Service's IT facilities.
- Safeguard the privacy and confidentiality of information received, transmitted or stored electronically.
- Ensure that the use of the Service's IT facilities complies with all Service policies and relevant government legislation.
- Provide employees with online information, resources and communication tools to support the effective operation of the Service.

The Board of Governance will:

Delegate operational responsibility and day-to-day management of the Service to the Nominated Supervisor/s. The Service Director and Service Manager will act as Nominated Supervisors for the Service.

Monitor the performance of the Association, including responsibilities contained in this procedure, through regular reporting and by ensuring appropriate resources are available to carry out the organisation's functions.

The Nominated Supervisor/s will:

Infrastructure

Ensure adequate provision of IT infrastructure and support to the Service including:

- The purchase and installation of IT equipment (including, computers, cameras and iPads, projectors, printers/photocopier).
- The installation and maintenance of an Internet connection (including wireless).
- The provision of email addresses for all employees and board members.
- Training in the use of software and the internet.
- Procedures for the regular backup of critical data and information at the Service.
- The provision of help desk support to employees.
- The provision of suitable access to the Service's IT facilities, as appropriate, to effectively manage and operate the Service.
- The engagement of a reputable IT company to oversee anti-virus and firewall software on Service computers, and to provide IT support when required.
- Software is kept up to date.

Security

Ensure that the use of the Service's IT complies with all relevant state and federal legislation and all Service policies and procedures.

Ensure that effective financial procedures and security measures are implemented where transactions are made using the Service's IT facilities, e.g. handling fee and invoice payments, and using online banking.

Provide clear procedures and protocols that outline the parameters for use of the Service's IT facilities.

Develop procedures to minimise unauthorised access, use and disclosure of information and data, which may include limiting access and passwords.

Develop procedures to ensure data, information (e.g. passwords) and equipment, are kept secure, and only disclosed to individuals where necessary e.g. to new employees or Board Members.

Social Media

Collaborate with team members to determine who has access to the Service social media accounts and who is responsible for uploading and sharing specific content and for responding to queries.

Ensure those with access to the Service social media accounts know how to use them appropriately and effectively.

Work to ensure images are secure and cannot be copied when sharing them via emails (e.g. electronic newsletter).

Ensure families are informed of this procedure during orientation, and how the Service social media platforms are used within the service.

Upon enrolment, ask parents/guardians to complete relevant paperwork that details permissions granted in relation to the sharing and use of their child's image, voice, creative work, etc.

Respectfully ask families to not take photos/videos at the Service that have other children in them, including other child/ren in the background.

Follow the *Employee Management Procedure* and/or *Code of Conduct if* there is a concern that a breach of this procedure has occurred.

All employees, volunteers and students will:

Adhere to and comply with this and all Service policies and procedures.

Infrastructure

Notify a member of Hawthorn Early Years Leadership Team of any damage, faults or loss of IT equipment.

Security

Comply with all relevant legislation and Service policies, protocols and procedures.

Understand that 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 prior approval from a nominated supervisor, as security of the information could be at risk.

Keep allocated passwords secure, including not sharing passwords.

Not share the Service's wireless password, unless there is a service provider on site that requires internet access.

Maintain the security of IT facilities belonging to the Service.

Only access accounts, data or files on the Service's computers where authorisation has been provided.

Use the Service's email, messaging and social media facilities for service-related and lawful activities only, and ensure no illegal or inappropriate material is transmitted at any time via any IT medium.

Use endpoint data storage devices (e.g. USB's) supplied by the Service for service-related business only, and ensure that this information is password protected from unauthorised access and use.

Ensure 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.

Ensure electronic files containing information about children and families are kept secure at all times and are password protected.

Log off after using a computer.

Not 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.

Appropriate usage of IT

Restrict the use of personal mobile phones or other personal devices to rostered breaks.

Not use, wear or take personal devices such as smart watches, phones, cameras or other IT devices into children's classrooms without the prior authorisation from a member of the senior leadership team.

Unacceptable & inappropriate use of IT facilities

Illegal and inappropriate use of IT 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.

All employees or other authorised users must refrain from:

- Exchanging any confidential or sensitive information held by the Service unless authorised as part of their duties.
- Creating or exchanging messages that are offensive, harassing, obscene or threatening.
- Creating, copying, transmitting or retransmitting chain emails spam or other unauthorised mass communication.
- Using IT facilities as a platform to gain unauthorised access to other systems.
- Carrying out activities that are illegal, inappropriate or offensive to fellow employees or the public. Such activities include, but are not limited to, material that ridicules/discriminates against others on the basis of race, nationality, creed, religion, ability/disability, gender or sexual orientation.
- Using IT facilities to access, download, create, store or distribute illegal, offensive, obscene or objectionable material (including pornography and sexually explicit material).
- Using IT facilities for personal financial gain or profit.
- Exchanging any confidential or sensitive information held by the Service unless authorised as part of their duties.
- Breaching copyright laws through making copies of, or transmitting, material or commercial software.
- Representing personal opinion as that of the Service.

Consequences of misuse

Individuals who use IT 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 Service will not defend or support any individual using the Service's IT facilities for an unlawful purpose.

Appropriate use of IT

Use technology as a teaching tool for the extension of the educational program by embedding it into the planned documentation of the classrooms program, as approved by the Educational Leader.

Follow the Early Childhood Australia (ECA) 'Statement on Young Children and Digital Technologies' for practice advise on the role and optimal use of technologies with, by and for young children.

Ensure portable devices used as part of the educational program are password protected and relevant to the age group.

Avoid the use of screen time for any child under the age of 3 years except when approved by the educational leader.

Ensure any material posted online (including personal and social media) meets service standards.

Be extremely mindful of those families and children who have relevant Court Orders in place regarding custody, and/or involvement with child protection services.

Adhere to the service's Code of Conduct and the ECA Code of Ethics.

Consequences of misuse

Employees who fail to adhere to this Procedure may be liable to lose/restriction of IT facilities, counselling, disciplinary action or dismissal.

Email Usage

Ensure that the content of emails and email addresses are always checked and double checked by the individual composing the email prior to sending.

Take care when sending emails to multiple recipients to avoid the inappropriate disclosure of email addresses to a whole group of recipients; blind copying (BCC) should be used wherever appropriate.

Always include a subject description in the subject line of emails.

Check emails regularly and respond if required as quickly as practicable.

Email Security

Demonstrate caution when opening files or launching programs that have been received as an attachment via email.

Not open attachments with unusual or suspicious filenames or if unsure of the sender to reduce the risks of viruses or malware.

Social Media Usage

Not ask to become 'friends' or actively seek social media connections with families. If an employee is connected with a family prior to the family or staff member commencing at the service, this needs to be disclosed to the Nominated Supervisor/s as a conflict of interests and a plan agreed upon to address concerns or mitigate risks.

Ensure they are aware of those children who have permission to appear on social media.

Conduct themselves professionally when using the service's social media and their own personal social media accounts.

Not reveal or share personal information of any team member, family or children.

Not post confidential information relating to the service, children or families.

Not use personal devices to take photographs of children.

Never share images of children on any platform without written consent from the parents/guardians.

Not post anything that is discriminatory, derogatory or defamatory.

Not access or engage with any material that is inappropriate or unlawful. This may include posts that are fraudulent, threatening, bullying, embarrassing, of a sexual nature, obscene, racist, sexist, defamatory or profane, whether obscured by symbols or not

Never engage in threatening or antagonistic conversation.

Not use social media for personal reasons whilst on duty.

Follow any guidance or direction from the Nominated Supervisor.

Report any misconduct in relation to this procedure or any other online behaviour that they are concerned or worried about to the Nominated Supervisor/s.

Parents/guardians will:

Not disclose the Service's confidential information.

Respect the privacy of the Service employees, children and other parents of the Service and not post or otherwise communicate content, which could be in breach the Information Privacy Act 2002 (Vic) and other applicable legislation (this may include the posting of photographs taken at the Service or at an external the Service function, unless only their child/ren appear in the photograph).

Refrain from sending or accepting 'friend requests' to/from employees of the Service or contacting employees via personal social media accounts.

Not include information sourced from the Service, which infringes the intellectual property rights of the Service or third parties.

Not make offensive, defamatory or derogatory comments about the Service, its employees, its Board or other families. This may amount to cyber-bullying or harassment amongst other things. If parents have any issues concerning the Service, including its management, employees, policies or values, these should be raised in the appropriate forum in accordance with the Complaints and Grievance Procedure.

Adhere to this procedure. Repeated failure to do so may result in a formal warning being issued by the Board in accordance with the Code of Conduct Procedure. This may ultimately result in care and education for your child/ren being suspended or withdrawn if the matter cannot be resolved and inappropriate behaviour continues.

Report any misconduct in relation to this procedure or any other online behaviour that they are concerned or worried about to the Nominated Supervisor/s.

See also:

- Governance and Management of Service Policy
- Privacy and Confidentially Procedure
- Complaints and Grievance Procedure
- Employee Performance Management Procedure
- Code of Conduct Procedure
- HEY's Philosophy in Action (previously named Pedagogical Strategy)