Digital Technologies Policy

Purpose:	To outline the basis on which students engage with the internet, on-line material and online activities and to comply with Ministerial Order 1359 To outline the school's governance, monitoring, and incident response processes
Scope:	School Coordinator (Principal), teachers (including casual relief staff), volunteers, parents and students
Implemented by:	School Coordinator (Principal), Teachers
Approved by:	Parent Group, LC Board
Communicated via:	School website, staff induction, enrolment agreement, Staff and Parent Group meetings
Reviewed:	Every two years or as legislative changes or improvements are identified

Definitions and Key Terms

Digital technologies are electronic tools, systems, devices and resources that generate, store or process data. Well known examples include social media, online games, productivity applications, multimedia, cloud based platforms, and mobile devices.

Digital learning is any type of learning that uses technology. It can happen across all curriculum learning areas and may be incidental to the learning or be an intentional part of the curriculum.

Cyberbullying consists of psychological bullying or harassment conveyed through an electronic medium such as a mobile phone, online platform or social media. It can be verbal (over the phone)

or written and can include threats of any nature, sharing of a person's private or personal information, harassment about a person's characteristics including race, sexual or gender identity, cultural background, mental health or other vulnerable characteristics, or sending inappropriate or prohibited content.

Social media encompasses digital platforms and technologies that facilitate the creation, sharing and interaction of content, enabling users to participate in social networking and communication. This includes:

- social networking sites (for example, TikTok, Snapchat, Instagram)
- video and photo sharing websites (for example, YouTube, Flickr)
- blogs, including corporate blogs and personal blogs (for example, WordPress, EduBlogs)
- micro-blogging (for example, X (formerly Twitter))
- forums, discussion boards and groups (for example, Reddit, Whirlpool, Discord)
- wikis (for example, PBWorks, Fandom)
- instant messaging (for example, Slack, WhatsApp, WeChat, Telegram, QQ).

Artificial Intelligence (AI) is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI is able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making and translation between languages. Examples of human-generated AI activities include:

- requests to summarize documents, information and publicly available resources
- requesting the generation of images based on specific characteristics and requirements
- engagement in questions and answers in a conversation style output
- the use of digital assistants such as Siri, Alexa and Google Assistant

Generative AI (GenAI) is a type of artificial intelligence that can create new content—such as text, images, audio, or code—by learning patterns from existing data. It uses models like large language models (LLMs) or generative adversarial networks (GANs) to produce original outputs that resemble human-created content.

Narrow AI is a type of artificial intelligence designed to perform a specific task or a limited range of tasks. It operates within a predefined scope and does not possess general reasoning or learning capabilities beyond its programmed function. Examples include voice assistants, spam filters, facial recognition systems, and recommendation algorithms.

Overview

Learning Co-operative values the use of digital technologies as tools to allow students to develop and demonstrate their understanding of concepts and content in all learning areas. We believe it is important that students are provided with regular and ongoing opportunities to develop their skills and understanding of the online world so that they can be confident, creative, thoughtful, empowered and safe users of this space.

In doing so, the school has a duty of care to provide a safe environment for students including online environments and this policy outlines the steps taken to promote the safety of students within the use of Digital Technologies during and outside of class time.

This policy also outlines the school's governance, monitoring, and incident response processes to manage and mitigate risks associated with the use of digital technologies.

Implementation Guidelines

Students in Levels 2-6 are provided opportunities to independently access digital technologies and as such will be required to sign a Digi-Tech Code of Practice. Students in Level 1 and Foundation will only access digital technologies under direct supervision, and as such are not required to sign a Digi-Tech Code of Practice.

The School will:

- Ensure staff and parents are provided with appropriate training, support and knowledge to assist them to identify and mitigate risks in online environments.
- Facilitate access for all students at our school to the programs, applications and services that are necessary, including access to the internet.
- Ensure any use of digital technologies in the school program has an appropriate educational purpose, mitigates privacy and child safety risks, and is consistent with community expectations.
- Provide regular lessons which outline strategies to enable students to keep themselves safe online by identifying risks and understanding how to seek support, understand online etiquette and what to do if they experience cyberbullying, grooming or other unwanted contact online.
- Ensure that the privacy of students, parents, staff and other users is recognized and respected at all times.

- Via the Enrolment Agreement, seek permission (or otherwise) for students to be photographed whilst enrolled at school for educational reporting, administrative and promotional purposes which may include online use. When it is necessary to identify students, only their first name will be used.
- Ensure the Coordinator works with the IT Committee to make sure all devices are running to an appropriate standard (current operating systems, updated browsers and appropriate security and filtering settings) with security and filtering settings which are appropriate for the users' age levels. -While full protection from inappropriate content cannot be guaranteed, the school maintains active filtering, monitoring and review processes to mitigate risk sand respond promptly to any breaches.

- Internet filtering systems will be reviewed at least once per term by the Co-ordinator and a summary provided to the Board in the Operations Report.

- Take every reasonable effort to ensure that information published on the Internet by students (or by the school featuring students) is done in a way that does not compromise the safety of students.
- Regularly review online activity and look for unusual patterns of usage, inappropriate content or other activity that is considered unnecessary or of risk.
- Ensure that Co-ordinator approval is sought for search histories and system logs to be reviewed where necessary to investigate suspected breaches of this policy
- Ensure the Coordinator approves all systems, platforms, devices and programs to ensure they are safe and fit for purpose.
- Have in place a Digi-Tech Code of Practice for students that is reviewed and endorsed by the Parent Group and Board with this policy.
- Work with families to understand the digital technology-related issues they are facing at home and support them with information and tools that help.
- Work to prevent, respond, and learn from issues or incidents relating to the use of digital technology, including cybersecurity incidents, cyberbullying and risks to child safety.
- Report all significant eSafety incidents to the Board in the Operations Report and review control measures following any breach.
- Ensure that the Child Safety Risk Register takes into account relevant, known and actual e-safety risks in our school's environment
- Follow the Child Safety Procurement Policy when entering into contracts with third-party suppliers to determine reasonable and appropriate requirements for the safety of students.

Staff and time on parents will:

- Support students to develop the skills necessary to filter, critically analyse, interpret and evaluate online content, in an ongoing and age appropriate way.
- Support students to develop and use known strategies for safe online activity.

- Identify and mitigate risks in the online and digital environments that students are accessing without compromising their right to privacy, access to information, social connections and learning opportunities.
- Understand that it is their responsibility to evaluate material, platforms, content and programs used in learning programs, prior to their use, to ensure they do not expose students to inappropriate or unlawful content.
- Remind students of the Digi-Tech Code of Practice when appropriate or required.
- Evaluate materials and programs and seek permission from the Coordinator prior to use. Staff must take into account the age and developmental stage of students, ensure they are appropriate, inclusive and respectful and meet the educational needs of the student group.
- Seek parent/guardian permission prior to creating online accounts for students, if the program or application falls outside of standard educational platforms that a parent would reasonably expect their child to have access to.
- Ensure the use of digital technologies supports student learning, and is safe, balanced and appropriate
- Supervise student's access to online social environments to ensure they are used in a safe and responsible manner.

- Report any known or suspected breaches of this policy or Digi-Tech Code of Practice to the Coordinator.

- Be aware that any personal devices that are used during school hours and activities, and at any time whilst using the school network are subject to policy.

Parents will:

- Provide guidance and support to their child to develop the necessary skills and knowledge to engage in online activities safely.
- Use built-in security features and parental controls on devices and apps to help manage their child's device access and restrict inappropriate content.
- Understand that we have clear and appropriate consequences when students breach the Digi-Tech Code of Practice.
- Notify a staff member if you become aware of any breaches of this policy or the Digi-Tech Code of Practice.
- Work collaboratively with the school to address any concerns impacting the safety or wellbeing of individuals in our school community.

Students will:

- Be required to understand, abide by and sign a Digital Technologies Code of Practice (if they are in Levels 2-6) which will be kept in the student's file.
- Be aware of their responsibility for notifying a teacher of any inappropriate material discovered so that access can be blocked and filters updated.
- Be made aware of their responsibility for notifying a teacher if they become aware of any breaches to this policy or the Digital Technologies Code of Practice.

- Ensure they do not bring their own electronic devices to school without permission from teaching staff.

Learning Co-operative does not condone the use of violence for the purposes of education or entertainment in online material, games or social environments. Only video games that students have created themselves can be played during school hours. If video games are played on school devices afterschool - for example during social game nights held at the Learning Co-operative- games must be age appropriate and where possible social rather than individual games.

Inappropriate or Unlawful Content

During school hours and activities, and at any time whilst using the school network or school devices, Students, Staff, Parents and Volunteers are strictly prohibited from using, storing or interacting with inappropriate or unlawful content. Such material, whether real or simulated, may include, but is not limited to;

- Content that infringes on another person's rights
- Content of a sexually explicit nature
- Content that promotes or instructs crime or violence

Concerns relating to the use of inappropriate or unlawful content should be raised immediately with the Coordinator.

Any accidental exposure to inappropriate content must be reported immediately to a staff member or the Coordinator so that filtering protections can be reviewed and strengthened.

Device Allocation and Use

- School-owned devices are to remain on site unless explicitly authorised by the Coordinator.
- A device sign-out register will be maintained for any authorised off-site use.
- Adults are not to use student-designated devices for personal purposes.

- Dedicated adult-use computers will be available in each learning space.
- Student devices and adult devices will be clearly distinguished.
- Devices are not to be used by students not currently enrolled at the school or by non-member adults.

Non School Time Safeguards

- Devices will be checked prior to school holiday periods to ensure filtering and security settings remain active.
- Devices shall remain on site during holidays and must be stored securely.
- Any inappropriate content identified during school holidays must be reported immediately to the Coordinator.

---

eSafety Incident Response Process

In the event of an eSafety breach or incident, or suspected breach, the school will:

- Immediately secure the device and prevent further access. If the device is not a school-owned device the Coordinator must be notified immediately. All relevant devices must remain secured until the investigation is complete.
- Provide wellbeing support to affected students where required.
- Notify the Coordinator as soon as practicable.
- Review the Protecting Children Policy to determine any actions that may be required based on the incident details.
- Conduct an internal investigation.
- Notify relevant authorities (e.g. Police, eSafety Commissioner, Child Protection) where required.
- Inform affected families in a timely and sensitive manner.
- Review and strengthen filtering and monitoring controls.
- Record the incident and actions taken.

- Report significant incidents to the Board.

Related Documentation

- Enrolment Agreement
- Education and Training Reform Act 2006 (Vic)
- Digital Technologies Code of Practice

Related Policies

- Privacy Policy
- Duty of Care Policy
- Child Safety & Wellbeing Policy