Acceptable use of Information and Communication Technologies for Students in Schools Policy

Last updated November 2021

Introduction

Schools are exciting places in which to teach and learn. Children naturally take advantage of developments in technologies to personalise and expand their learning opportunities, and teachers provide rich learning environments for children as they engage with people and resources, locally and globally.

In this dynamic and connected world of communication and learning, schools need to ensure that such opportunities do not place young people at risk. Many of these risks are not new and educators are familiar with strategies and processes that maximise learning opportunities and outcomes, while minimising risk to children's safety and wellbeing.

The information contained in this policy:

- Establishes the context for effective use of information and communication technologies for students at Good Shepherd Lutheran School;
- Outlines procedures that will both protect and inform students and their parents;
- Ensures students, staff and parents are aware of their responsibilities.

This policy should be read in conjunction with Good Shepherd Lutheran School's other policies particularly the Behaviour Management, Anti – Bullying and Child Protection policies.

Relevant Legislation, Standards and Frameworks

Education and Early Childhood Services (Registration and Standards) Act 2011
http://www.legislation.sa.gov.au

Children's Protection Act 1993
http://www.legislation.sa.gov.au

DECD Cyber – Safety: Keeping children safe in a connected world – Guidelines for preschools and schools
http://www.decs.sa.gov.au/docs/documents

Responding to Online Safety Incidents in South Australian Schools – Guidelines for Staff Working in Educational Settings
Education.EngagementAndWellbeing@sa.gov.au

DECD Protective Practices for Staff in their Interactions with Children
http://www.decs.sa.gov.au/docs/documents

National safe Schools Framework, Safe Schools (Australian Government) website
http://www.deewr.gov.au/Schooling/NationalSafeSchools/Pages/overview.aspx

Copyright Act 1968
http://www.legislation.gov.au

Privacy Act 1988
http://www.legislation.gov.au

Definitions

A safe and supportive school – 'in a safe and supportive school, the risk from all types of harm is minimised, diversity is valued and all members of the school community feel respected and included and can be confident that they will receive support in the face of any threats to their safety and wellbeing'. National Safe Schools Framework, updated 2013, Education Services Australia.

Children and students – all learners enrolled at Good Shepherd Lutheran School.

Parents – natural parents, legal guardians and caregivers.

ICTs – information and communication technologies.

Cyber – safety – the safe use of the internet and ICT equipment/devices, including mobile phones.

Cyber bullying – bullying which uses e-technology as a means of victimising others. It is the use of an internet service or mobile technologies – such as email, chat room discussion groups, instant messaging, webpages or SMS (text messaging) – with the intention of harming another person. Examples include communications that seek to intimidate, control, manipulate, put down or humiliate the recipient.

Digital footprints – are traces left behind by someone's activity in a digital environment. These traces can be analysed by a network manager or the police.

Sexting – is where a person takes a sexually explicit digital photograph of him or herself or of someone else and sends it as an MMS and SMS via a mobile phone. These images can then be posted on the internet or forwarded electronically to other people. Once posted on the internet these images can leave a permanent digital footprint and can be accessed at any time in the future. It is illegal to take sexual photos or videos of children and young people.

Social networking – sites that offer people new and varied ways to communicate via the internet, whether through their computer or mobile phone. These sites allow people to easily and simply create their own online page or profile and to construct and display an online network of contacts, often called 'friends'. Users are able to build a network of connections that they can display as a list of friends. These friends may be offline actual friends or acquaintances, or people they know or have 'met' only online, and with whom they have no other link. Social networking sites are not limited to messaging, communicating and displaying networks. Nearly all sites allow users to post photos, video and often music on their profiles and share them with others.

School ICT – refers to the school's computer network, internet access facilities, computers and other ICT equipment/devices as outlined below.

ICT equipment/devices – includes but is not limited to computers (such as desktops, laptops, netbooks, personal digital assistants (PDAs), storage devices such as universal serial bus (USB) and flash memory devices, compact discs (CDs), digital video discs (DVDs), iPods, MP3 players, cameras (such as video and digital cameras and webcams), all types of mobile phones, gaming consoles, video and audio players/receivers (such as portable CD and DVD players), and any other similar technologies.

Inappropriate material – means material that deals with matters such as sex, cruelty or violence in a manner that is likely to be injurious to children or incompatible with a school environment.

E – crime – occurs when computers or other electronic communication equipment/devices (e.g. Internet, mobile phones) are used to commit an offence, are targeted in an offence, or act as a storage device in an offence.

Malware – is an abbreviation of 'malicious software' and means software programs designed to cause damage and other unwanted actions on a computer system. Common examples include computer viruses, worms, spyware and trojans.

Personal use – means all non-work related use, and includes internet usage and private emails.

School related activity – includes but is not limited to an excursion, camp, sporting or cultural event, wherever its location.

Guiding Principles

In alignment with the National Safe Schools Framework, Good Shepherd Lutheran School commits to the following guiding principles:

- Affirming the rights of all members of the school community to feel safe and be safe at school.
- Acknowledging that being safe and supported at school is essential for student wellbeing and effective learning.
- Accepting responsibility for developing and sustaining safe and supportive learning and teaching communities that also fulfil a school's child protection responsibilities.
- Encouraging the active participation of all school community members in developing and maintaining a safe school community where diversity is valued.
- Actively supporting young people to develop understanding and skills to keep themselves and others safe.
- Empowering students by involving them in the decision making and resolution processes.
- Developing a safe school community through a whole school approach.

Acceptable Use of Information and Communication Technologies for Students in Schools

In order to keep our students safe, Good Shepherd Lutheran School has developed a Student ICT User Agreement which reflects this policy. Students and their caregivers receive a copy and are required to sign it before accessing ICTs each year.
In addition to the user agreement, students are explicitly taught how to use Information and Communication Technologies in a way that keeps themselves and others safe. They are also encouraged to report breaches of this policy to a staff member.

Acceptable and Unacceptable Use

Acceptable use includes:

- Use of the school's network in connection with curricular, co – curricular or pastoral activities.
- Sending or receiving emails using an appropriate school-based email account.
- Using the internet in connection with teaching and learning and along guidelines established by teaching staff.

Unacceptable actions or intent may include:

- Bullying, invading privacy, defaming or harassing individuals through messaging, emails, posting of blogs, wikis and/or images on web-based sites.
- Unlawful activity (e.g. breaching copyright laws and licence agreements, hacking accounts of other users, accessing passwords or transgressing school protective measures).
- Accessing, possessing, displaying or exchanging inappropriate material (e.g. pornographic, racial, discriminatory, political or violent material).
- Spamming or sending bulk emails, including electronic chain mail.
- Damaging or modifying the computer network (e.g. by introducing viruses, hacking, changing software settings, installing software, or damaging/modifying hardware).
- Using another person's password, disclosing a password to someone or impersonating someone.
- Accessing or manipulating another person's storage folder or files.
- Wasting network resources through excessive internet downloads.
- Deliberate misrepresentation of the school.
- Downloading information from the school network in order to provide it to an unauthorised third party.
- Disabling, interfering with or overloading any computer system or protective measure.
- Downloading, transferring or viewing inappropriate files or subscribing to inappropriate email lists.
- Disclosing personal details of yourself or others.
- Using the school network to contravene any school rules.
- Posting defamatory, obscene, libellous or generally inappropriate content.
- Seeking friendships with teachers via social networking pages.

Policy Breach

A breach of this policy can be defined as a student not meeting the requirements of the Student ICT User Agreement or is considered an unacceptable action as per 'Unacceptable Actions and Intent' within this policy. When a breach has been identified, the following processes will apply:

- Teacher investigates and determines course of action. If another member of staff becomes aware of a breach, it will first be directed to the student's class teacher.
- The teacher can deal with minor breaches independently, using the school's behaviour management policy as a guide.
- Depending on the nature of the breach, the ICT Administrator and/or Principal will also be informed and become involved.

Typical reasons for involving the ICT Administrator include breaches whereby equipment is damaged. The ICT Administrator can also provide assistance by contacting ICT support to change settings to protect the safety of other users or to investigate possible breaches.

Typical reasons for reporting to the Principal involve serious breaches that:

- Require further investigation.
- Involves parent communication.
- Have legal implications (e.g. copyright, transmission or receipt of inappropriate internet material).
- Involves all cases of bullying and/or harassment.

Consequences of Breaching the Policy

All breaches of this policy will be taken seriously. There are a range of consequences that may be enforced depending on the nature and seriousness of the breach. Such consequences may include:

- A restorative process whereby a breach has impacted another student.
- A time of reflection with the Principal.
- Restricted/loss of access to ICTs for a period of time.
- Restricted/loss of access to the Internet.
- Payment for broken equipment.

Breaches of criminal law may also be matters for the police.

Legal Liability, Legal Obligations and Privileged Information

When individuals choose to go public with opinions online, they are legally responsible for their commentary. Individuals can be held personally liable for any commentary deemed to be defamatory, obscene, proprietary or libellous. Students should exercise caution with regards to exaggeration, colourful language, guesswork, obscenity, copyrighted materials, legal conclusions and derogatory remarks or characterisations.

The internet does not provide the privacy or control assumed by many users. Students should appreciate that no matter what protections they place around access to their personal sites their digital postings are still at risk of reaching an unintended audience. Students should be aware of the following expectations in considering their use of social networking sites:

- Have considered the information and images of them available on their sites and are confident that these represent them appropriately.
- Comments on their site about their school, friends or staff, if published, would not cause hurt or embarrassment to others, risk claims of libel, or harm the reputation of their school, their friends or staff.

Sexual harassment or acts that amount to criminal or sexual assault may be referred to the police. Students, or parents of students, who have been subjected to such acts may take legal action. Acts that constitute an e-crime could be referred to SAPOL.

Acts where there is suspicion of child protection issues must be referred to the Child Abuse Report Line (13 14 78) in line with mandatory reporting requirements.

Students should exercise good judgement and common sense when creating and distributing email messages. The school and/or individuals may be liable for defamatory, misleading or deceptive statements contained in email messages, and may also be liable for the disclosure of information which is confidential or which constitutes personal information as defined by the Privacy Act 1988 (Cth).

Students are required to be at least 13 years of age to be able to create online accounts as per the terms and conditions of the individual site.

Privacy

Electronic communication is not a secure means of communication. While every attempt is made by the school to ensure the security of its resources, users must be aware that their security is not guaranteed, particularly when communicating to an external party. The sender should consider the confidentiality of the material they intend to send when choosing the appropriate means of communicating.

Electronic communication and work created via the school's network is not private, and the school may access their storage files to check for compliance with the policy. The school may also access real – time information including what is displayed on screens.

The school cannot guarantee the confidentiality of on-line communication by users of the school's network.

Any email sent from the school's network is the property of the school and will necessarily reflect on the school.

Implementation Responsibilities

The **Principal** will:

- Seek to ensure that Christian Values, attitudes and behaviour are modelled and supported in a digital environment.
- Commit to developing a school learning community which is safe, inclusive, conducive to learning and free from cyber harassment and bullying.
- Inform new members of the school community of the philosophy and expectations of this policy.
- Ensure all users of the school's computer network sign an ICT Acceptable Use Agreement.
- Provide professional learning opportunities for staff to gain knowledge, understanding and skills in enhancing student learning through ICTs and responsible behaviour in a digital environment.
- Facilitate, where appropriate, the involvement of other agencies to support staff and families in the effective and safe use of digital technologies.
- Review this policy regularly ensuring it meets the requirements of other relevant policies and legal obligations.

The **ICT Administrator** will:

- Review user statistics and filtering tools, involving ICT support to block access to inappropriate sites and filter specific words and phrases that could be used for inappropriate searches or messages where necessary.
- Maintain and update the network's anti-virus software.
- Manage and monitor user accounts and network use.

- Inform the Principal of any instances of misuse of the internet, email service, or other ICT equipment.
- Maintain a closed email environment in which students can only receive emails from domains approved by staff.
- Ensure that the software installed by the school is covered by the necessary licences.

Students will:
- Read, discuss with parents, sign and follow the Student ICT User Agreement.
- Take responsibility for reporting inappropriate usage of ICT in the school community.

The **Staff** will:
- Discuss the contents of this policy before permitting students to use ICT facilities, regularly reminding students of the contents of the user agreement they have signed, and encouraging them to make positive use of ICT.
- Develop student ICTs skills and knowledge:
    - Teach students how to access and use the ICT equipment correctly.
    - Guide students in effective strategies for searching and using the internet.
    - Provide explicit cyber-safety instruction as outlined in school curriculum documents.
- Provide adequate supervision for students whilst accessing ICTs.
- Observe copyright laws and educate students to correctly reference works; and follow up on and report breaches of this policy as soon as practicable.

Parents will support this policy by:
- Discussing the ICT Guidelines with their child and explaining why they are important.
- Supporting the school's cyber-safety program by emphasising the need to follow cyber-safety strategies.
- Contacting the principal or delegate to discuss any questions and/or report any breaches about cyber-safety and/or this policy.
- Covering the cost of damages to ICT that their child has caused.
- Supporting the ethos of the school by modelling a positive online presence.

Policy due for review November 2024