Cyber-Safety Policy and Guidelines

July 2022

Summary

This policy applies to Community Language Schools SA and all member schools.

Table 1: Document Details

Policy Number	**ES39**
Related Policies	ES01: Child Safe Environments Policy and Procedures ES02: Risk Management Policy ES2B: General Incident Report Form ES05: School Personnel Code of Conduct Policy ES06: Student Code of Conduct Policy ES07: Enrolment Policy and Procedures ES07A: Student Online Enrolment Form ES10: Personal Information and Photograph Release Policy ES11: Communication Policy and Guidelines ES15: Sexual Misconduct Policy and Guidelines ES16: Adult Students attending Community Language Schools Policy ES20: Data and Information Policy ES21: Copyright Policy ES35: Behaviour Support Policy and Procedures ES38: Bullying and Harassment Policy and Procedure ES39A: Cyber-Safety and Use of ICTs Agreement Form ES39B: Cyber-Safety in School User Agreement ES39C: Code of Conduct in an Online Learning Environment Agreement ES40: Special Needs Policy ES41: Gender Identity Policy and Guidelines
Version	2.2
Created by	CLSSA Policy Officer
Reviewed by	CLSSA Executive Officer
Applies to	All Community Language Schools
Key Words	Cyber-safety; Access and security; Cyber-bullying; Information Communication Technology (ICT); Personal Electronic Devices (PEDs); Peripheral Device; Inappropriate material; Social media; Sexting; Acceptable use guidelines.
Status	Approved
Approved By	CLSSA Board *(Administrative updates approved by Executive Officer)*
Approval Date	July 2022
Review Date	December 2023
Notes	Administrative and content update

Table 2: Revision Record

Date	Version	Revision Description
February 2017	1.0	New policy developed
30th June 2019	2.0	• Amend policy to make it generic by replacing individual school details with "Community Language Schools." Change names of State Government departments; added relevant policy names and numbers • Changes in 'Created By' and 'Reviewed By' in Table 1; Changed Contents to Table of Contents; Reformatting of table and titles; Added new key words; Changed Other Relevant Documents to References and Other Documentation; Formatting of policy
18th January 2021	2.1	• Added Policies to Related Policies (Table 1) • Amend content in Policy • Separated Cyber-Safety in School User Agreement from **ES39A**- is now **ES39B** • Created **ES39C** • Amend content in Cyber-Safety User Agreement • Added 'School Administrator and/or' to Responsibilities
December 2021	2.2	• Changed policy name from 'Cyber-Safety Policy' to 'Cyber-Safety Policy and Guidelines' • Changed the heading of 'Camera' to 'Camera, Video Recorders, Mobile Phones and Tablets/iPads' and also amended the content under this heading • Added content in 'Personal ICT Devices' • Added content in 'Parent/Caregiver Agreement' in **ES39A** • Added content in in **ES39B**
July 2022	2.2	• Administrative and content update

Table of Contents

Cyber-Safety Policy and Guidelines 1
Summary 1
Table 1: Document Details 1
Table 2: Revision Record 2
Cyber Safety Policy and Guidelines 4
Introduction 4
Definitions 4
Policy 5
Student Responsibilities 5
Access and Security 6
Appropriate Behaviour and Use 6
Sexting 7
Cameras, video recorders, mobile phones, tablets/ iPads 7
Personal ICT Devices 7
Online incidents of inappropriate behaviour affecting students 8
Removing inappropriate content 9

Reporting inappropriate online content 9
Cyber Safety User Agreement 10
Responsibilities 10
References and Other Documentation 11

Cyber Safety Policy and Guidelines

Introduction

The Internet, Information Communication Technologies (ICT) and educational technologies provides an opportunity to enhance the teaching and learning at Community Language School. Students will use ICT in a variety of ways including class work, homework, research, collaborating with peers, sharing ideas and communication with others. Students may be required to communicate through the use of ICT with other students, teaching staff, parents, and community members. The effective and appropriate use of ICT allows school personnel and students at Community Language Schools to strengthen communication, streamline administrative tasks, and engage students in learning.

This policy outlines the guidelines for access and security, appropriate behaviour and use when using ICT, cyberbullying and the cyber safety user agreement. This policy is based on information from the Department of Education, Cyber Safety Keeping Children Safe, Facebook, The Australian Government: Office of the Children's eSafety Commissioner and the Enhancing Online Safety for Children Act 2015.

Definitions

Cyber Safety refers to the safe and appropriate use of the Internet and ICT equipment

Cyber Bullying is bullying which uses technology as a means of victimising others. It is the use of an Internet service or mobile technologies such as e-mail, chat room discussion groups, instant messaging, social media, webpages or SMS (text messaging) with the intention of harming another person. Examples include, but not limited to, communications that seek to intimidate, control, manipulate, put down or humiliate the recipient.

ICT is an abbreviation for Information Communication Technology and is a term use to describe any communication device, networks, application, storage, mobile devices, personal electronic devices, peripheral devices, hardware, and software.

Personal Electronic Devices (PEDs) refers to but is not limited to laptops, tablets, smart phones, smart watches which are owned by individual users and brought to the school

Peripheral Device is an item that can be connected to a computer such as printer, scanner, speaker, and microphone

Inappropriate Material refers to material that deals with matters such as sex, cruelty or violence in a manner that is likely to be harmful to children or incompatible within the Community Language School environment.

Social Media: has the sole or primary purpose of enabling interactions between two or more people, post or share material for social purposes and the service allows users to link or interact with some or all of the other users.

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 or 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 be accessed at any time in the future. It is illegal to take sexual photos or videos of children and young people.

Policy

Education has changed dramatically, with the distinctive rise of e-learning, whereby teaching is undertaken remotely and on digital platforms. Since the use of the Internet, mobile devices and ICT at Community Language Schools have increased, there should be a responsible use of technology by students with the guidance from teaching staff which will provide a secure and safe learning environment. All school personnel and students will be issued with an Acceptable Use of ICT Agreement (refer Cyber-Safety User Agreement) and once signed consent has been returned to the Community Language School, learners will be able to use ICT accordingly.

While every reasonable effort is made by the school to prevent children's exposure to inappropriate content when using the Internet, it is not possible to completely eliminate the risk of such exposure. Community Language Schools will use the following three key principles in teaching and learning activities involving ICT:

- Engage Positively
- Know your online World
- Choose Consciously

When students engage positively they are exercising their rights and responsibilities as a digital citizen and at the same time respecting the rights of others. Knowing about the online world that students engage in and interactive with, will assist students at school to understand how to appropriately use ICT. A conscious choice is when a student makes well informed decisions about what they do online, how they interact and know how to protect themselves.

Student's Responsibilities

It is the responsibility of students to:

- Only use devices after getting permission from the teaching staff/ volunteer that is in-charge of their classroom
- Abide by the acceptable use agreement
- Report inappropriate behaviour and material to a teaching staff or Principal
- Be aware that a breach of this policy may result in disciplinary action in line with **ES35:** Behaviour Support Policy and Procedures

- Communicate through internet and online communication services is related to learning
- Only download or upload material for educational purposes
- Manage and care for their own devices, and equipment
- Keep passwords confidential, and change when prompted, or when known by another user
- Use passwords that are not obvious or easily guessed.
- Not disable settings for virus protection, spam and filtering that have been applied
- Not knowingly forward an email that contains a virus, spam, unsolicited advertising material, hoax emails or a message sent to them in confidence

Access and Security

The following section outlines Community Language School's policy on using ICT appropriately, the security measures that are required and what to do in the event that a student or students are exposed to inappropriate content online

Students may use the Internet during school hours only for learning related activities that are approved by the teaching staff. Students must not cause interference or disruption to other people or equipment and students must not access or distribute inappropriate material. These includes:

- Distributing spam messages or chain letters
- Accessing or distributing malicious, offensive or harassing material, including jokes and images
- Bullying, harassing, defaming or giving offence to other people
- Spreading any form of malicious software such as viruses, worms
- Accessing files, information systems, communications, devices or resources without permission.
- Using for financial gain
- Using non-approved file sharing technologies
- Using for non-educational related streaming videos or audio
- Using for religious or political lobbying
- Downloading or sharing non-educational material

Appropriate Behaviour and Use

Students will be made aware of behaviour that is unacceptable or inappropriate when using ICT. At no time is sexting, sending inappropriate material to another student or person is acceptable. The following sections outline the policy and guidelines for sexting, the use of cameras and online incidents of inappropriate behaviour affecting students.

Sexting

Sexting can have serious social and legal consequences. If a student has sent a picture or video that they regret sending, students are encouraged to request that the picture or video be deleted from all sources. Students are required to report the issue so further action can be taken. The safest thing students can do is to never share something that they don't want other people seeing. Students are reminded that if somebody asks them to share something that they are not comfortable with, that they have the right to say no.

If an adult has asked a child to send a picture or video that is of a sexual nature, and a teaching staff, volunteer, school personnel or Principal of the Community Language School become aware of the situation, they are required by law to call the Child Abuse Report Line (CARL) on 131 478. Refer to **ES01:** Child Safe Environments Policy

Cameras, video recorders, mobile phones, tablets/ iPads

Cameras, video recorders, phones, tablets or electronic devices that can record audio and/or video must not be used in private spaces or isolated areas including, but not limited to, toilets, storage rooms, or behind school buildings. Photographs or images produced by students or school personnel may be considered as 'personal information' and may be subjected to Copyright. Teaching staff and students must not use any material for purposes unless they have the informed consent of the creator.

Students are not allowed to take photos or record anything without the permission of the teaching staff. If a member of school community believes that their privacy has been invaded they will first need to consult the Principal or School Administrator. If the issue is not resolved, the Principal or School Administrator can forward the issue to CLSSA's Executive Officer. Refer to **ES10:** Personal Information and Photograph Release Policy and **ES20:** Data and Information Policy

Personal ICT Devices

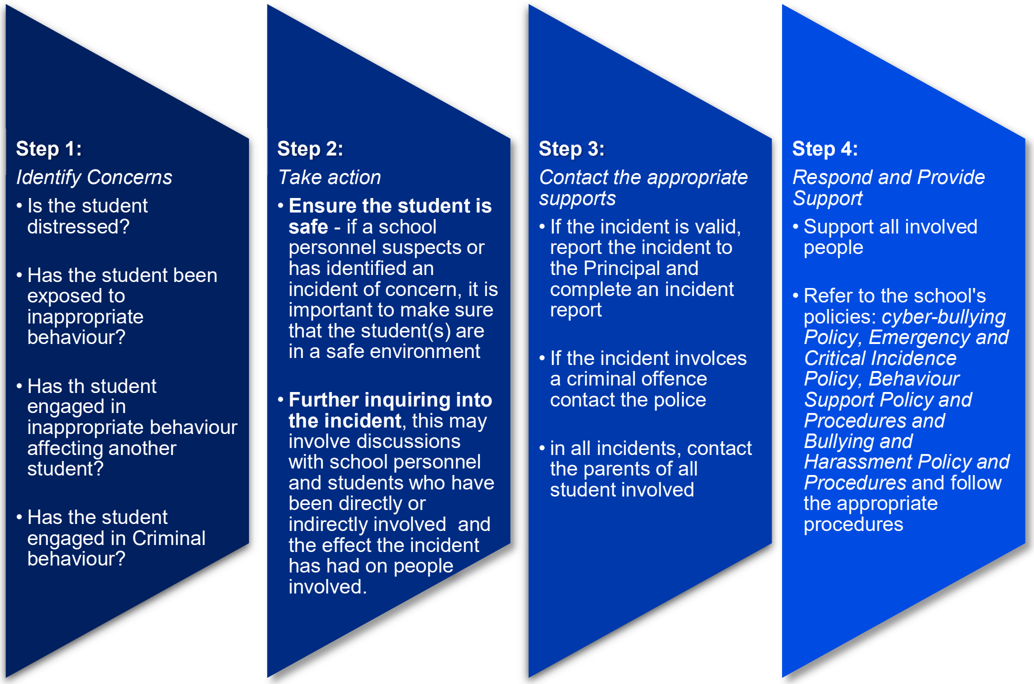
Community Language Schools requires school personnel and students to bring their own device to school. Students must adhere to **ES39A**: Acceptable Use of ICT Equipment and Devices Agreement, **ES39B**: Cyber-Safety in School User Agreement and **ES39C**: Code of Conduct in an Online Learning Environment Agreement while using their personal device in the school. Schools will not take responsibility for any damage, theft or lost devices. Devices are not permitted to be used during break times and must be securely stored. Devices are not required on excursions unless prior arrangement has been made. Any device used at a Community Language School may be subjected to an inspection by the school Principal.

Online incidents of inappropriate behaviour affecting students

An incident of concern may involve a single activity or a serious of incidents. Community Language Schools have a duty of care to keep all students safe including during online learning activities. An incident where a student has been exposed to inappropriate behaviour online may cause the student(s) distress, psychological or emotional harm. The **ES08A**: Incident, Injury, Trauma and Illness Form needs to be completed in the event of any only incident of inappropriate behaviour affecting students. Inappropriate content for students includes, but not limited to:

- Words or images that personally attack or defame an individual
- Content that threatens, harasses, discriminates, menaces or causes offence
- A fake social media profile of an individual or school
- Any images, photographs, videos, animations, depictions of nudity, pornography or child abuse
- Any images, photographs, videos, animations, depictions of violence that is real or simulated including domestic violence,
- Content that is illegal, gives instructions of illegal activity or advocates terrorists activities
- Content that is obscene
- Content that depicts the promotion, or use of drugs and/or alcohol
- Material that is harmful to students under the age of 18

In the event that a student at a Community Language School has been exposed to or engaged in inappropriate behaviour online, the school will take actions as shown in the diagram below:



Step 1:
Identify Concerns
- Is the student distressed?
- Has the student been exposed to inappropriate behaviour?
- Has th student engaged in inappropriate behaviour affecting another student?
- Has the student engaged in Criminal behaviour?

Step 2:
Take action
- **Ensure the student is safe** - if a school personnel suspects or has identified an incident of concern, it is important to make sure that the student(s) are in a safe environment
- **Further inquiring into the incident**, this may involve discussions with school personnel and students who have been directly or indirectly involved and the effect the incident has had on people involved.

Step 3:
Contact the appropriate supports
- If the incident is valid, report the incident to the Principal and complete an incident report
- If the incident invoices a criminal offence contact the police
- in all incidents, contact the parents of all student involved

Step 4:
Respond and Provide Support
- Support all involved people
- Refer to the school's policies: *cyber-bullying Policy, Emergency and Critical Incidence Policy, Behaviour Support Policy and Procedures and Bullying and Harassment Policy and Procedures* and follow the appropriate procedures

Diagram 1: Responding to Online incidents of inappropriate behaviour affecting students

Removing inappropriate content

Community Language Schools will take the following measures if inappropriate material has been identified:

- If the person responsible for publishing the inappropriate content is known, that person will be asked to remove and delete the content from all sources.
  - If the person responsible is a student, it is up to the community language school's discretion to act on the student
  - If the person responsible is a school personnel, their involvement in the community language school will be reviewed and an exclusion from the community language school will be a consideration
- If the person responsible for publishing the inappropriate content is NOT known then the school will:
  - Refer to the term and conditions of individual social media platforms (see Table 3 for more details).
  - Inform parents of the incident
  - If required, to call police

Table 3: How to report inappropriate content or material on various social media platforms

Social Media Platform	Process	Link
Facebook	Use the report link near the post, photo or comment to report the inappropriate content to Facebook	Report something | Facebook Help Centre
Instagram	Tap report and follow the instructions	Abuse and spam | Instagram Help Centre Use this link if you do not have an Instagram account: Instagram Help Centre
Twitter	Tap the more icon then select report and click it's abusive or harmful. Follow the instructions to provide more details	How to report abusive behavior on Twitter | Twitter Help
Snapchat	Block or delete the user by tapping the gear near the screen and either block or delete	Snapchat Support
Pinterest	Click on the pin and click report, select the reason for reporting. Follow the instructions to provide more details.	Report something on Pinterest | Pinterest help

Reporting inappropriate online content

Community Language Schools will adhere to provisions for making complaints about a child that has received cyber-bullying material as outlined in The *Enhancing Online Safety for Children Act*

2015. Community Language Schools will report offensive or illegal content to the Officer of the Children's eSafety Commissioner if the student, teaching staff or Principal has reason to believe that a student enrolled at a Community Language School was "or is the target of cyber-bullying material that has been, or is being, provided on a particular social media service or relevant electronic service, the child may make a complaint to the Commissioner about the matter." (Australian Government, 2016, p. 14.)

Community Language Schools will report offensive or illegal content to the Office of the Children's eSafety Commissioner at - What is illegal and restricted online content? | eSafety Commissioner

Any complaint made to The Children's eSafety Commissioner must be made within a reasonable time and must be accompanied by evidence. Evidence could include a receipt from a social media service that the issue has been reported. Alternatively if no receipt is provided by the social media service, a screen shot of the inappropriate or offensive material or a statutory declaration.

Community Language Schools will ensure that students who have received cyber-bullying, offensive, obscene or inappropriate material will be provided with the contact details of services including Kids Helpline via the website at https://kidshelpline.com.au or phone 1800 55 1800. After an incident has occurred, the school will review the Cyber-bullying Policy and Guidelines and update accordingly.

Cyber Safety User Agreement

All school personnel and students will be issued with **ES39A**: Cyber Safety and Use of ICT Agreements and once signed consent has been returned to the Community Language School, learners will be able to use ICT (School personnel don't need to sign page 2 of **ES39A**- Acceptable Use of ICT Equipment and Devices Agreement)

ES39B: Cyber-Safety in School User Agreement should also be signed and returned to the Community Language School for students to enable students to use the Internet, mobile devices and ICT in school. **ES39C**: Code of Conduct in an Online Learning Environment Agreement is to be signed if and/or when the Community Language School is to conduct e-learning via Zoom, Google Classroom or any other online platform for e-learning.

Responsibilities

It is the responsibility of the School Administrator and/or Principal to ensure that:

- all virus protection software is up-to-date
- students are aware of safe practices when using ICTs

- all students enrolled at a Community Language School have signed and returned the Cyber-Safety User agreement.
- Any report made to the eSafety Commissioner is made within a reasonable time and provide any necessary evidence.
- Students are referred to services that can help with the aftermath.

It is the responsibility of the teaching staff or Volunteer to:

- Record the incident, if possible, taking screenshots of the inappropriate material, witness accounts and observations, including date, time, location and who was involved
  - The Teaching staff and/or Principal will then follow the procedures for managing behaviours as outline in the **ES35**: Behaviour Support Policy and Procedures
- Record the process taken to resolve the incident including steps taken to remove the inappropriate material, mediation attempts, discussions with students and parents, consequences used for students who were instigators

References and Other Documentation

- Facebook (2017) Safety Resources Staying Safe | Facebook Help Centre
- Office of the Children's eSafety Commissioner Report offensive or illegal content - What is illegal and restricted online content? | eSafety Commissioner
- Office of the Children's eSafety Commission Report Cyber-Bullying - What is serious online abuse? | eSafety Commissioner
- The Australian Government Office of the Australian Information Commissioner. The Privacy Complaint Checker - before-you-lodge-a-complaint-with-us - Home (oaic.gov.au)
- The Australian Government Federal Register of Legislation (11 July 2016). Enhancing Online Safety for Children Act 2015 - Enhancing Online Safety for Children Act 2015 (legislation.gov.au)
- The Australian Government: The Office of the Children's eSafety Commissioner. Digital Citizenship - Video library for educators | eSafety Commissioner