**Nhill Lutheran School**

ABN 16 649 962 149

2 Mackay Street, Nhill 3418

*Phone:* (03) 5391 2144

*Fax*: (03) 5391 1220

*email*: admin@nls.vic.edu.au

 www.nhillls.vic.edu.au

CYBER SAFETY POLICY

**RATIONALE:**

Nhill Lutheran School places a high priority on providing internet facilities and electronic learning devices which will benefit student learning outcomes and the effective operation of the school. However, it recognises that the presence of these technologies in the learning environment (some provided partly or wholly by the school and some privately owned by staff, students and other members of the school community), can also facilitate anti-social, inappropriate, and even illegal behaviour and activities. The School aims, therefore, to maximise the benefits of these technologies while at the same time to minimise the dangers and manage the risks.

The Policy is written in light of the Mission Statement of the School: *Nhill Lutheran School provides a quality education in a caring Christian environment.*

**POLICY:**

1. Nhill Lutheran School will develop and maintain rigorous and effective cyber-safety practices which aim to maximise the benefits of the internet and electronic learning devices to student learning and to the effective operation of the school, while minimising and managing any risks;

2. These practices will aim to not only maintain a cyber-safe school environment but also to address the needs of students and other members of the school community to receive education about the safe and responsible use of present and developing information and communication technologies;

3. Associated issues include the need for relevant education about cyber-safety for the school community, implications for the design and delivery of the curriculum, professional development and training, disciplinary responses appropriate to breaches of cyber-safety, the availability of appropriate pastoral support, and potential employment issues. Cyber-safety is a key component of the ICT Curriculum delivered at each Year level.

4. Teaching resources will be provided to ensure that teachers have access to current and appropriate curriculum materials. All teachers will have a responsibility to ensure safe online practices within their class and take every opportunity to engage students in relevant dialogue about current cyber-safety issues.

5. Nhill Lutheran School takes its responsibility to provide robust policy, guidelines and education for students in relation to what is deemed acceptable and appropriate online behaviours seriously. These include:

* The school name, logo and/or uniform must not be used in any way which would result in a negative impact for the school and its community.
* Except under teacher direction (eg Seesaw), students must not post photos of either themselves and/or other students which clearly identify them as a member of the Nhill Lutheran School community, nor post photos taken during any school sanctioned activity. This includes away from school events such as sports days and camps.
* Members of the school community have a responsibility to ensure that all online communications are in keeping with the school’s expectations in relation to appropriate and respectful interactions with teaching and non-teaching staff.
* Facebook and other social media platforms prohibit the use of its site by persons under the age of 13 years.
* Staff members are not to have a student as a Facebook friend, or on other social media platforms, while a student is enrolled at the school and for a period of 2 years after a student has left the school.
* Students will not post inappropriate comments about individual staff members or other students which if said in person would result in disciplinary action being taken.
* Neither the school’s network nor the broader internet when used for school purposes (whether accessed at school or away from school, either during or after school hours, via any application) may be used for any purpose other than that for which it was designed. This includes cyber-bullying, harassment, taking, sending or receiving naked or sexually explicit images (sexting) and other misuses of technology.
* Students are not to search for clips on video streaming services such as YouTube while at school to avoid the risk of inappropriate images or texts appearing on the screen. The teacher or teacher aide will have the responsibility of searching and loading video clips which they must do without the students being able to view the screen.
* The clip from YouTube or other video streaming service shown to students is to be enlarged to full screen before it is shown. This will avoid students being exposed to inappropriate advertising that often appears around the reduced screen.
* The school will have an internet filtering system in place for all curriculum computers to safeguard against students viewing potentially harmful images or texts.
* Students will only have access to websites that have been screened by the teacher.
* Teachers are not to google images while students can view the screen to avoid the risk of inappropriate images or messages being seen by students.
* Students are not allowed to google websites or images apart from those already screened by the teacher to ensure there are no inappropriate images or messages.

*“Cyber-bullying is a way of delivering covert psychological bullying. It uses information and communication technologies to support deliberate, repeated and hostile behaviour, by an individual or group that is intended to harm others”* (Belsey, 2007)

1. Cyber-bullying includes but is not limited to the following misuses of technology:

* harassing
* teasing
* intimidating
* threatening another person by sending or posting inappropriate and hurtful material
* verbal abuse
* humiliating someone
* spreading rumours or lies
* setting up fake profiles
* excluding others
* e-mail messages
* text messages
* phone messages
* digital pictures or images
* website postings (including blogs).

The forwarding of private emails, messages, pictures or videos or otherwise inappropriately communicating personal or private information belonging to another person or logging on and pretending to be someone else as well as sending sexually explicit images (sexting) and intentionally excluding others from an online group all constitute cyber-bullying. If this occurs with school related tasks, either during school time or after school hours, it will constitute a breach of school policy and as a result the student concerned will be subject to disciplinary action. Students must be aware that in certain circumstances where a crime has been committed, they may also be subject to a criminal investigation by Police over which the school will have no control.

Students who feel that they have been the victims of such misuse of technology should save or screenshot and store the offending material on their computer, mobile phone or other device. They should then print a copy of the material and immediately report the incident to a teacher, parent/caregiver. Staff who may have been cyber-bullied or threatened online should immediately report such incidents to the Principal. Students and staff should also block the person to prevent further contact or access.

All reports of cyber-bullying and other technology misuses will be investigated fully and may result in a notification to Police where the school is legally obliged to do so. Sanctions may include, but are not limited to, the loss of computer privileges, suspension or expulsion from the school.

*Students and parents/caregivers are required to sign the Cyber-safety agreement at the commencement of each year.*

This policy is to be read in conjunction with Social Media Policy and Staff Code of Conduct.

DATE: May 2024

FOR REVIEW: May 2027