Anti-Cyberbullying Policy

Hartland International School
مدرسة هارتلاند انترناشيونال

This policy includes definitions for and the guidelines related to procedures involved in the prevention of cyberbullying at Hartland International School. It also outlines procedures for dealing with such cases should they occur.

References to Hartland children should be read as Pupils in the Primary phase and Students in the Secondary phase of the school and are interchangeable.

September 2024

Purpose

This Policy outlines the commitment of Hartland International School to create a safe and supportive environment for all students. We recognise the impact of cyber bullying on students' well-being and academic performance, and we are dedicated to preventing and addressing such behaviour effectively.

Scope of the Policy

This policy recognises that students have access to a variety of different technologies at school and in their personal lives. The scope of this policy covers the following areas:

- Where a school student or staff member is the victim or alleged perpetrator of cyberbullying
- Where cyberbullying occurs on school premises or during the school day
- Where school devices, technology or network access are mis-used with intent to conduct cyberbullying
- Where a school student or staff member is the victim of cyberbullying through an anonymous source

Definition of Cyberbullying

Cyberbullying is defined as any form of bullying that occurs through digital devices, including but not limited to:

- Flaming – e.g. posting or sending negative, hurtful or vulgar messages digitally.
- Harassment – e.g. repeatedly sending hurtful or unwanted messages digitally to another person.
- Cyberstalking – e.g. repeatedly sending threatening or intimidating messages digitally that cause fear.
- Impersonation – e.g. deliberately adopting the persona of another person through forced access to their online account or through creation of a fake account.
- Degradation – e.g. deliberately sharing or posting of gossip, rumours or other information about a person with intent to cause harm to their image or reputation.
- Exclusion - e.g. deliberately creating online discussion or groups digitally with the intent to exclude another.
- Out-ing e.g. digitally sharing information, images or other personal information about another person without permission.

Monitoring and Device Management

To promote a safe digital environment, the school employs the following measures:

- All school iPADS are monitored using Mosyle which limits functionality and restricts access to content.
- All students in Years 5-13 are required to bring their own device to school and must sign the Hartland Acceptable Use Agreement prior to receiving their login details.
- All parents of students receive a copy of the Bring Your Own Device (BYOD) Policy which clearly outlines school procedures and is available on the school website.
- Student Wi-Fi Network access is limited to a single source which is controlled by Fortinet, a firewall system that restricts internet access and is controlled by the school.
- The Meraki firewall system logs staff and student connections to different access points in the school.
- Each student has a unique username and password to the school Wi-Fi, at any point their internet access, search history and browser history can be accessed.
- Students must hand in mobile phones at the beginning of each school day in Years 6-11 to ensure that restricted websites, applications or content cannot be access through use of mobile data.

Roles and Responsibilities

This policy recognises the important role that all members of the school community play in creating a safe and supportive online environment.

Students

Students are responsible for their own conduct online. All students have a responsibility to use technology safely and receive regular education and support in being a responsible digital citizen.

Staff

Staff are responsible for the monitoring of student activity online during and between lessons. Staff should always be vigilant and ensure that any use of technology is supervised.

Parents and Carers

Parents and carers are responsible for monitoring and controlling their child's access to and use of technology outside of school hours. Parents and carers are encouraged to talk openly with their children about responsible and safe use of the internet and report any concerns regarding cyberbullying to the school.

Preventative Measures

The school implements various proactive strategies to prevent cyberbullying, including:

- Annual online safety lessons conducted through the Computer Science curriculum which focus on raising awareness and developing digital citizenship.
- Awareness campaigns including Safer Internet Day and National Online Safety Week.
- Regular teaching and training through tutor time activities and assemblies.

Response Procedures

In the event of a reported cyberbullying incident, the following procedures will be followed:

- Staff members are trained to respond promptly to any reports of cyberbullying through reporting to DSL.
- A thorough investigation will be conducted by designated staff, including gathering evidence and documenting all relevant details.
- The school will provide support services for victims, including counselling and guidance.
- Appropriate disciplinary measures will be taken against those found responsible for cyberbullying in accordance with the Hartland Behaviour for Learning Policy and Anti-Bullying Policy.

Date for next Review

September 2025

Relationship to other policies, guidelines and statements

- Behaviour for Learning Policy
- Anti Bullying Policy
- Bring Your Own Device (BYOD) Policy

Signed.....Date.....

School Principal