1. Objective

The Cyber Safety Policy is designed to ensure that all staff, students, parents and carers understand that there is zero tolerance to cyberbullying.

This Policy is to be implemented in conjunction with the Anti-Bullying and Non-Violence Policy.

2. Scope

This Policy applies to all students enrolled at Cheshire School, their parents, guardians and carers, staff as well as to other relevant members of the community such as volunteers and visitors.

3. Context and Guiding Principles

A person is bullied when someone or a group of people, deliberately upset or hurt another person or damage their physical or online property, reputation or social acceptance on more than one occasion. There is an imbalance of power in incidents of bullying with the bully or bullies having more power at the time due to age, size, status or other reasons. People who use the internet, email, intranets, phones, social networks or similar technologies to bully others are cyberbullies.

Bullying in any form is unacceptable. Bullying that is carried out through an internet service, such as email, chat room, discussion group or instant messaging or through mobile phone technologies such as short messaging services (SMS) is cyberbullying. Cyberbullying can be very destructive and will not be tolerated at any level, and serious consequences exist for students who choose to bully others.

At Cheshire School:

- Every child and young person has a right to be safe.
- Staff have a duty of care to take reasonable steps to protect students from any harm that should have reasonably been foreseen, including those that may be encountered within the online learning environment.
- Learning technologies are used ethically and responsibly in the school environment
- A whole school approach is adopted to address cyber safety.

4. Definitions

Word	Definition
Acceptable Use Agreement	• These are documents created by the school to outline what is acceptable behaviour when using computer facilities and other technologies such as mobile phones.
Cyber abuse	• This is behaviour that uses technology to threaten, intimidate, harass or humiliate someone – with the intent to hurt them socially, psychologically or even physically. Cyber abuse can take place on social media, through online chat and messaging services, text messages, emails, on message boards and in online forums that allow people to comment quickly.
Cyberbullying	• This is the use of technology to bully someone – to deliberately

	and repeatedly engage in hostile behaviour to hurt them socially, psychologically or even physically. It is generally used to refer to the online abuse of children and young people. Groups and individuals can be both the perpetrators and targets of cyberbullying. Cyberbullying can take place on social media, through online chat and massaging services, text messages, emails, on message boards and in online forums that allow people to comment publicly.
Inappropriate Content	• This refers to material that is illegal or developmentally inappropriate that is shared or accessed online. This can include posting of inappropriate images or comments. It can also include accessing online platforms that contain explicit material.

5.   Policy

Cheshire School expects:

- an acceptable standard of behaviour from all children when using ALL technologies within school premises or whilst using school based communication systems
- that all parents and students to have discussed, signed and returned the school's Acceptable Use Agreement
- the ICT equipment provided is used for educational purposes
- that all students, parents and teachers will abide by school determined netiquette;
- that any breaches of this code will result in investigation and possible withdrawal of privileges.

Acceptable Behaviour and Use
Whilst using the Cheshire School network:

- students must abide by the expectations outlined in the school's Acceptable Use Agreement
- students will be accountable for any inappropriate actions (e.g. bullying, accessing or sending inappropriate material);
- students may use the Internet only for learning related activities that are approved by a teacher;
- students must not cause interference or disruption to other people or equipment;2
- no private student devices will be allowed access.

The Head of School is responsible for:

- ensuring that the Acceptable Use Agreement is implemented and signed annually
- reinforcing with the school community cyber safe practices
- alerting everyone within the school community of the signs and evidence of cyberbullying
- informing the school community that they have a responsibility to report cyberbullying

to staff, whether as an observer or as a victim

- ensuring that all reported incidents of cyberbullying are investigated appropriately and that support is provided to both victims and perpetrators
- seeking parental, carers, staff and student support in ensuring at all times cyber safe behaviour
- ensuring that parents, guardians and carers, staff, students and the wider school community are made aware of the types of cyberbullying and its legal and hurtful ramifications. Staff will be regularly reminded of their duty of care regarding protection of students form all forms of bullying.

Staff are responsible for:

- observing a duty of care - this means taking reasonable care to protect students from foreseeable risk of injury when using the internet for educational purposes
- providing appropriate supervision for students when accessing the internet and other web-related collaborative tools
- designing and implementing appropriate programs and procedures to ensure the safety of students
- teaching students about dangerous situations, materials and practices
- fulfilling their responsibilities to deliver child protection curriculum within whole of site planning for such delivery
- teaching strategies for personal safety and advise students that they should not reveal personal or identifying information including names, addresses, financial details (e.g. credit card); telephone numbers or images (video or photographic) of themselves or others.

Parents, Guardians and Carers are responsible for:

- reading and discussing with their child the school's Acceptable Use Agreement
- returning the signed Acceptable Use Agreement to the school
- supporting the school's cyber safety programs by encouraging their child to follow the cyber safety rules, and to always ask the teacher if they are unsure about any use of ICT
- contacting the school to discuss any questions they might have about cyber safety and/or the school's Acceptable Use Agreement.

Digital Technologies - Students are responsible for:

- communicating respectfully and politely with what they post, write
- be kind to friends and classmates and think about how the things they do or say online may make others feel
- do not send mean or bullying messages or forward them to other people
- create and present their own work and when copying something from online, advising by sharing the website link to acknowledge the creator
- stop and think about what the post and share on line

- will note share or post the link (or password) to video conferencing meetings, with other offline in public communications or online or public websites or social media forums

- use spaces or sites that are appropriate and if not sure ask a trusted adult for help

- protect their friends' personal details such as their full names, birthdays, school names, addresses and phone numbers

- speak to a trusted adult if they see something that makes me feel upset or if they need help

- speak to a trusted adult if someone is unkind to them or they know someone else is upset or scared

- don't deliberately search for something rude or violent

- turn off or close the screen if I see something I don't like and tell a trusted adult

- are careful with the equipment they use.

6. Associated Procedures

- 05.008 Enrolment Policy and Procedure
- 001.2 Child Safe Policy and Procedure
- 05.006c Anti-Bullying and Non-Violence Policy
- Parent Handbook
- Student Code of Conduct
- OH&S Incident Report Form

7. Relevant Legislation Sources

- The Children's Services Act 1996
- The Federal Disability Discrimination Act 1992
- The Victorian Equal Opportunity Act 2010
- The Occupational Health and Safety Act 2004
- Education and Training Reform Act 2006
- Information Privacy Act 2000

8. Other Resources

- Bully Stoppers
- DET Classroom Resources
- eSmart
- The eSafety Commissioner