STUDENT ICT Acceptable Use Policy

At North Haven School we use the internet, computers, iPads and Chromebooks for learning tasks and information gathering. We want students to be safe while they are using these resources, and also responsible for what they do.

Purpose

Our school is committed to providing a cyber-safe learning environment for all students. This agreement must be read and acknowledged by all students prior to the use of any school ICT or department ICT facilities or services. This agreement applies to all on-site technology, software, loaned devices and personal devices connecting to the school network (including laptops, tablets, Chromebooks, cameras and mobile phones).

Cyber-safety refers to the safe use of the Internet and ICT equipment/devices, including mobile phones.

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 email, chat room discussion groups, instant messaging, web pages or SMS (text messaging) - with the intention of harming another person.

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

ICT equipment/devices includes computers (such as desktops, iPads, tablets, laptops, Chromebooks, PDAs), storage devices (such as USB and flash memory devices, iPods, MP3 players), cameras (such as video and digital cameras and webcams), all types of mobile phones, gaming consoles, video and audio players/receivers, 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 or preschool environment.

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

Student Users of North Haven School ICT facilities:

North Haven School offers Internet access for student use.

An acceptable use policy outlines to users the types of inappropriate behaviours when using the department's ICT facilities and services. The policy is to be read, acknowledged and implemented by an agreement by all users. A signed copy of the agreement must be retained in the student's file for reference if needed.

For younger children (R-2), parents or guardians agree to ensure their child is aware of personal safety strategies. Older children (3-6) may take responsibility for their own actions by agreeing to use the ICT facilities in a responsible manner, but with parent or guardians acknowledging the responsibility their child undertakes.

While every reasonable effort is made by schools and the Department for Education (DfE) administrators to prevent children's exposure to inappropriate content when using the department's online services, it is not possible to completely eliminate the risk of such exposure. In particular, the DfE cannot filter Internet content accessed by children from home, from other locations away from school or on mobile devices owned by your child. The DfE recommends the use of appropriate Internet filtering software.

Educational Purpose

Internet facilities have been established for educational purposes, including classroom activities and self directed research. Students are expected to follow the rules about acceptable use of computers and related equipment.

All students will have access to the Internet's information resources through classroom laptops, school iPads and student's own Chromebooks. Students will have email access only under their teacher's direct supervision (Year 3-6).

Access to the internet is to be used primarily for department related business purposes, e.g. communications related to department business, authorised professional development and activities related to a person's duties.

Interference or disruption to other networks or shared-system users, services or equipment will not be tolerated.

At NHS we have an Acceptable Use Agreement outlining the expectations of students when using digital technologies

Unacceptable usage includes but is not limited to:

Students connecting to the network either on a school issued device or personal device must comply with the following:

- Students must only use their own assigned computer network account.
- Students must not share personal information about themselves or other students with third parties, including their username or passwords. It is the responsibility of all students to protect their own password and not divulge it to another person. If a student or staff member knows or suspects an account has been used by another person, the account holder must notify the classroom teacher immediately.
- School ICT assets must not be used to access or share inappropriate content online, including sexually explicit materials, obscene depictions, harmful materials, illegal activities, profane or abusive language, or content that other students may find offensive.
- Web and email content filtering must not be circumvented to access content that has been deemed inappropriate for students.
- Copyright materials (including games and movies) must not be illegally downloaded onto or accessed using school or department issued ICT assets.
- When using online communities, users must communicate kindly and respectfully at all times. Students must not participate in harassing or bullying other students online.
- Students must not forward chain letters, spam or other unsolicited communications.
- Students must not participate in business activities that is not staff approved or done so as part of curriculum learning.
- All students must immediately report suspicious activity or violations of this policy to a staff member.
- Students must not violate any state or federal laws, including purchase of illegal items or substances, criminal activities punishable by law, etc.
- Students must not take photos or videos of another individual without their consent.
- Students must not use school or department ICT assets to stream large volumes of data unless in the course of curriculum activities (e.g. streaming services such as Netflix, online gaming etc).
- Students must not install unapproved software on school or department issued devices.

Under certain circumstances social networking sites may be beneficial for learning. However, in most instances social networking sites can be a distraction and potentially unsafe. Therefore, students must seek permission from their teacher or parent/caregiver before accessing social networking sites at home and school.

School internet filters block many social networking sites. Students using social networking sites without permission during lessons will be subject to consequences. Students are reminded to use cyber-safe strategies and use the internet in a safe and ethical manner. Students must not be part of whole class / cohort online chat forums such as Messenger and Snapchat.

Parents/Caregivers and teachers are asked to actively monitor online behaviour and encourage children to follow cyber safe strategies at home and at school.

Consequences of breach

Our school reserves the right to monitor use of ICT assets used by students. Students that misuse assets or use assets in an inappropriate manner may have their access revoked.

All messages created, sent or retrieved on the school's network are the property of the school. The school reserves the right to access and monitor all messages and files on the computer system, as necessary and appropriate. Communications including text and images may be required to be disclosed to law enforcement and other third parties without the consent of the sender.

This acceptable use policy enforces consequences for inappropriate behaviour, and in extreme cases prosecutions. The school reserves the right to restrict/remove access of personally owned mobile devices to the intranet, internet, email or other network facilities to ensure the integrity and security of the network and to provide a safe working and learning environment for all network users. The misuse of personally owned mobile devices may result in disciplinary action which includes, but is not limited to, the withdrawal of access to school supplied services, referral to South Australian Police and in extreme cases prosecutions.

Confiscated devices must be handed over with the student's cooperation and never physically removed from the student's possession. If a student refuses to follow a reasonable instruction to put away or hand in their device, escalating responses should be provided in line with the school's behaviour support policy.

- Parent/carers can be asked to attend the school to collect their child's confiscated device. But if they're not able to attend on that same day, the device will be returned to the student before they go home.

Behaviour incidents outside of school hours or off school grounds

The Principal may (but is not required to) suspend, exclude or expel students for behaviours that happen outside of school hours or off school grounds where there is a reasonable connection between the student's behaviour, the school community and school relationships. This may include behaviour:

- that happens on the way to and from school
- when the student is wearing the school uniform or is representing the school, for example school camps, sporting carnivals or on the school bus
- in person or online towards another student or school staff, at home or in the community, for example, threatening, harassing or bullying behaviour
- during camps or excursions that are provided by external agencies under authority of the school.

This policy will be communicated to our school community in the following ways:

- Available publicly on our school's website
- Discussed at parent information nights/sessions
- Included in transition and enrolment packs
- Included as annual reference in school newsletter
- Made available in hard copy from school administration upon request

References:	*Acceptable use policies for schools, preschools and children's services' sites standard* *Code of Ethics for the South Australian public sector* *Practical guide for the use of email and the internet guideline* *Student-use-of-mobile-phones-and-personal-devices-at NHS Policy*

Reviewed: May 2024 Governing Council approved: 14 / 05 / 2024