

INTERNET SAFETY POLICY

**NAG 5
NO. 505**

Purpose

The aim of this policy is to ensure safe use of the internet by all members of the school community. St Heliers School recognises that the internet is a valuable tool for teaching and learning and can be a useful resource. However, due to their nature or content some sites on the internet are not suitable for viewing in a school community. The school endeavours, as much as is practicable, to ensure that everyone using its online facilities, can do so safely and securely.

Guidelines

1. The Principal, in consultation with the e-Learning team, teachers, parents and other appropriate staff, has the prime responsibility for decisions related to internet access.
2. The school will regulate and monitor internet access. This will be used to block sites deemed unsuitable for viewing at school due to inappropriate content. Examples of this are auction or shopping sites, social networking sites, gaming sites or sites containing swearing, adult content, substance abuse or material of a violent nature. It will also be used to regulate file downloads, for example, large files types and e-mail attachments which may carry viruses.
3. All devices owned or leased by the school will be subject to SSL inspection (Secure Sockets Layer), and may have the school's Network for learning SSL Certificate installed. The same applies to any device connected to the school network that is intended for student use. For example, student devices (BYOD) or devices supplied by agencies to supplement the learning of students with special needs.
4. The internet safety officer appointed will be the leader of the e-Learning team.
5. N4L in conjunction with the internet safety officer has initial responsibility for setting access to internet sites, monitoring the sites visited and search engine terms used throughout the school. If any member of staff has a concern about access to a particular site or group of sites, they should inform the internet safety officer.
6. Individuals or groups may have reasons for requesting access to a blocked group of sites. In this situation they may ask the internet safety officer to have the block removed from the individual/group account(s). If they are not happy with the internet safety officer's decision, they may apply to the Principal.
7. The school recognises the need for children to be aware of internet safety issues in order to use the internet securely and responsibly. Children will learn digital citizenship skills in order to use the internet in a way which will keep themselves and their computer safe.
8. The school has no responsibility (financial or other) for damage or loss of students own (BYOD) devices.
9. Appendix 1 (attached) details the rules for students using the internet.
10. Appendix 2 (attached) each student will have a Consent to Publish Child's Learning form completed by caregivers. This form outlines whether the caregiver gives consent to have learning shared online. Forms are stored for reference throughout the children's time at school.

Appendix I

Rules for using the Internet – To be displayed in each classroom

When using the internet, students should follow the values of St Heliers School, in particular being **responsible, honest, and respectful** and showing **care**.

1. Students must not use the internet without an adult present. This includes BYOD devices.
2. Students must not give out identifying personal information including their, or any other person's, name, address, phone number or photo over the internet.
3. Students must not send or post emails, blog messages or attachments over the internet unless they have previously been approved by a teacher.
4. Students must not download attachments, files, programmes, videos or music without prior approval of a teacher. Students should be aware of copyright and legal responsibilities involved in downloading or copying information from the internet.
5. Students communicating online are expected to uphold St Heliers School rules and values, and report any comments which breach these values.
6. Students must not use social media, video conferencing software, or private email accounts without teacher permission and supervision. Students using video conferencing are expected to uphold St Heliers School rules and values and report any breaches of these values.
7. Students who are bringing their own devices to school must not allow other students to use their device.
8. Students must tell their teacher if they find anything on the internet which they consider inappropriate or upsetting.

Appendix 2

Consent to Publish Child's Learning

e-Learning is teaching and learning that is facilitated by or supported through the appropriate use of information and communication technologies and is an integral part of today's and tomorrow's teaching and learning.

Classes, groups and individuals will sometimes share their learning with the school community and with others in the educational community via the internet and other media. This means, from time to time, a child's learning will be shared online including photos, blogs, videos and written work. Online learning will only ever be for educational purposes.

Privacy and safety is very important. No identifying information such as address, surname or personal email address will be shared. At all times students are expected to uphold the school values and follow the school rules when using any digital technology.

Consent for your child's learning to be shared as described above is sought for the duration of his/her enrolment at St Heliers School.

If you need clarification of any of the above, please do not hesitate to contact the school office and they will direct you to the appropriate staff member.

Thank you.

Sean Valvoi
Principal

Consent to Publish Child's Learning

I give my consent for _____ to share his/her learning online whilst at St Heliers School

or

I do not give my consent for _____ to share his/her learning online whilst at St Heliers School

Signed: *Full name:*

Relationship to student: Date: