St Scholastica's Primary School

DIGITAL TECHNOLOGIES POLICY

This policy must be read in the context of St Scholastica's Child-Safe Policy.

Rationale:

Our students use technology to learn. Technology is essential to facilitate the creative problem solving, information fluency, and collaboration that we see in today's society. While we want our students to be active contributors in our connected world, we also want them to **be safe, legal, and responsible**. This policy supports our vision of technology use and upholds in our students a strong sense **of digital citizenship**.

We use technology to:

- facilitate creativity and innovation
- support communication and collaboration
- extend research and information fluency

We create a safe online environment for everyone. Filtering software keeps unwanted sites off our computers and adults supervise our students' computer activities at school. Children are taught how to respond to unwanted material that may elude the filters.

Being a Digital Citizen

At St. Scholastica's we use information and technology in safe, legal and responsible ways. We embrace the following conditions or facets of being a digital citizen.

- **Respect Yourself**. I will select online names that are appropriate, I will consider the information and images that I post online.
- **Protect Yourself**. I will not publish my personal details, contact details or a schedule of my activities.
- **Respect Others**. I will not use technologies to bully or tease other people. I will not access or alter another person's online material
- **Protect Others**. I will protect others by reporting abuse and not forwarding inappropriate materials or communications.
- **Respect Intellectual Property**. I will suitably cite any and all use of websites, books, images, media, etc.
- **Protect Intellectual Property**. I will request to use the software and media others produce.

Procedures

Vandalism and Harassment

Vandalism is defined as any malicious attempt to harm, modify, and/or destroy data of another user, Internet or other networks. This includes, but is not limited to, the uploading or creating of computer viruses.

Harassment is defined as the persistent annoyance of another user, or the interference of another user's work. Harassment includes, but is not limited to, the sending of unwanted mail. This area is further developed within the School Student Wellbeing policies.

Encounter of Controversial Material

Users may encounter material that is controversial and which users, parents, teachers or administrators may consider inappropriate or offensive. However, on a global network, it is impossible to screen or filter content of all data. It is the user's responsibility not to initiate access to such material or to distribute such material by copying, storing or printing. Students are guided to report any such material to a teacher immediately.

Security

If a security problem is identified on the Internet it must be reported to the system administrator. The problem must not be demonstrated to others.

Attempts to log on as the system administrator may result in the cancellation of user privileges.

Any user identified as a security risk for having a history of problems with their computer systems may be denied access to the computer facilities and Internet at St. Timothy's Primary School.

Student protocols:

Students are encouraged to talk to a teacher or another adult if:

- They need help online
- They are not sure what they should be doing on the Internet
- They come across sites which are not suitable for our school
- Someone writes something they don't like, or makes them or their friends feel uncomfortable or asks them to provide information that I know is private
- They feel that the welfare of other students at the school is being threatened by online activities

We recommend the students:

- Do not use their own name, but develop an online name and use avatars
- Do not share personal details or limit the details to one aspect (first name or surname only)
- Keep password protection on any spaces or accounts they have and protect that password
- Do not allow anyone they don't know to join their chat or collaborative space
- are reminded that any image or comment they put on the Internet is now public (anyone can see, change or use it)

The school will:

- Do its best to enhance learning through the safe use of ICT. This includes working to restrict access to inappropriate, illegal or harmful material on the Internet or school ICT equipment / devices at school or at school –related activities.
- Work with children and their families to encourage and develop an understanding of the importance of cybersafety through education designed to complement and support the user agreement initiative. This includes providing children with strategies to keep them safe in cyberspace.
    - Keep a copy of this signed agreement on file.
    - Respond to any breaches of this agreement in an appropriate manner.
    - Welcome enquiries from parents or students about cybersafety issues.
    - Conduct parent information sessions
- Model correct cybersafe behaviours through the use of class blogs and management of student blogs.
- Participate in cybersafe initiatives to strengthen the cybersafe message.

In response to breaches of this policy, the school will follow the following procedure:

Minor events

- Warn the student and remind them of appropriate on-line behaviours and discuss the consequences of their behaviour. Remove access for a short period (for example, lesson length

More serious breaches and repeated minor events

- Restrict the access to the school network and internet for a period of time (relative to the extent of the breach), whilst notifying the parent in writing of the nature of the breach and the school's response.

Evaluation:

This policy will be reviewed as part of the school's review cycle.

Related policies:

Digital Technology Police
Acceptable Use of the Internet Policy
Acceptable User Agreement
Student Wellbeing Policy
Prevention of Bullying Behaviour
Internet Usage Policy