



IRAMOO PRIMARY SCHOOL No. 5152

eSmart-CyberSafety POLICY

Rationale:

It is important for the school to provide a safe and friendly environment for students and staff and to foster the school values of Respect, Responsibility, and Relationships. All persons have a legal right to be protected from harassment and discrimination and a responsibility to use technology appropriately.

CyberSafety and Ethics refers to appropriate use of technology ensuring users behave safely when online. This includes awareness of:

- **Cyberbullying** – a form of bullying which is carried out through an internet service such as email, chat room, online social networking, instant messaging or web pages. It also includes bullying through mobile phone technologies such as SMS and it may involve text or images
- **Protecting privacy** - posting private information or pictures online
- **Respecting property** - copyright issues related to downloading or unauthorized use of information found online
- **Being proactive** and reporting concerns
- **Copyright/other legal requirements**

Aims:

- To provide a safe environment at school for students to use online resources for learning
- To develop awareness of safe and ethical Internet use
- To develop an awareness of how to deal with CyberSafety issues at school and home
- To encourage appropriate and safe use of technology

Implementation:

School:

The school will adopt procedures to promote a CyberSafe learning environment by:

- making the school community aware of the school's position on CyberSafety
- regularly reminding teachers about the school's eSmart- CyberSafety policy
- making staff aware of their responsibilities under the DET Acceptable Use Policy
- using an Internet Service Provider to effectively filter, track and regulate school internet traffic
- monitoring the school's computer network and identifying potential problems
- ensuring all students from Grade 3 to Grade 6 have signed the student DIGITAL TECHNOLOGIES STUDENT ACCEPTABLE USE AGREEMENT annually
- conducting lessons on CyberSafety and ethics by classroom teachers and ICT teacher
- establishing a school CyberSafety contact person
- providing online resources for staff and parents outlining common Cybersafety issues
- providing Professional Development opportunities for staff on CyberSafety and ethics issues

- making staff, students and parents aware of the Iramoo Portable Electronic Devices Policy
- reinforcing positive technology behaviours

Parents/Guardian:

Parents are required to support our School eSmart-CyberSafety Policy by:

- reading and signing the Digital Technologies Student Acceptable Use Agreement and discussing it with their child/ren
- monitoring student use of Technology (email, social networking, internet access, online games, mobile phone use) at home
- reinforcing the school's eSmart-CyberSafety Policy in the home environment
- where appropriate reporting CyberSafety concerns to the classroom teacher and/or school CyberSafety officer
- discourage use of inappropriate technologies

Students:

Students have a responsibility to use all technologies in a safe and appropriate manner by:

- reading, signing, and adhering to the Digital Technologies Student Acceptable Use Agreement
- adhering to the Iramoo Portable Electronic Devices Policy
- reporting any CyberSafety concerns to the appropriate adult
- using technology at school and home in an appropriate manner

Consequences:

If a student breaches the school's eSmart-CyberSafety Policy the following consequences will apply.

- offenders will be spoken to by the appropriate person and incidents will be investigated and documented
- if necessary parents will be notified and authorities alerted
- offenders and victims will be offered counseling and support if required
- offenders will be denied access to school network for a period of time
- if a student persists to offend parents will be contacted and consequences implemented consistent with the school's Student Code of Conduct
 - Consequences for students will be individually based and may involve, exclusion from ICT class, restricted use of IT at school, exclusion from yard, withdrawal of privileges
 - ongoing monitoring of identified offenders.

Resources Required:

- Funding for appropriate Internet Service Provider which will provide services in line with the policy.

Evaluation:

- Number of reported and/or detected breaches of the student AUA
- Monitoring of Internet use by staff
- This policy will be reviewed as part of the school's three-year review cycle