**Policy: Protection from Dangers of the Global Information
Network (the Internet)**

**Introduction:
protection from dangers of the global information network** includes the measures taken by Elite APS to:

•Protect students from exposure to online harmful materials, communications
and behaviors, by means that shall include the use of a reliable filtering system
that alerts the School’s Principal and teachers to inappropriate Internet usage
by students and prevents students from gaining access to offensive and other
unsuitable websites.
•Prevent unauthorized persons from gaining access to School data.
**Cyber-bullying** is defined as the use of electronic and information devices, such as email, instant messages, text messages, mobile phones and websites to send or post messages or images that may harm an individual or a group.

**Rational:**•To set out the Council’s requirement that students are protected from morally
offensive, inappropriate or other undesirable content on the Internet and
preventing access to websites that contain such materials.
•To educate students on the proper use of the Internet and sharing of personal
information.
•To promote good practices in using secure Internet systems.

**Policy Statement:**The School should use a filtering system for websites in order to monitor students’ usage and to ensure that they are protected from morally and socially inappropriate materials. In this regard, Principal prepares, implements and regularly reviews an Internet Security Policy which includes, for example, the following points:
•Installing an Internet filtering and security system in order to monitor students’
Internet use and to ensure their protection from online materials that are not
consistent with morality, decency or public order.
•Prohibiting the viewing or downloading of any inappropriate material
(offensive or immoral remarks, jokes or any other comments that may offend
someone based on their physical or mental disability, age, religion, social status,
political affiliations, and ethnicity).
•Monitoring Internet usage by the School’s IT department.
•Having teachers and librarians take an active role in protecting students from
the dangers of the Internet and monitoring websites accessed by students as
well as monitoring students during a School trip in case they have access to
electronic devices that are connected to the Internet.

•Guiding students in on-line activities that will support learning outcomes,
depending on the students’ age and maturity.
•Prohibiting the use of the Internet to attempt unauthorized access to other
computers, information or prohibited services.
•Not to open e-mails or attachments from unknown sources.
•Prohibiting the downloading or copying of copyrighted material, including
software, books, articles, etc., which are not licensed for use
by the School.
•Prohibiting the undertaking of any activity that may introduce viruses or other
malicious software to the School’s network.
All Schools shall ensure that the personal information placed on the School’s Internet and intranet is secure, even for a password-protected website.
Schools should endeavor to communicate with the Council using available technologies (e.g. email, etc.), ensure safe and confidential lines of communication.

**ROLES AND RESPONSIBILITIES:**

**Elite APS** will:
- Ensure that an effective and reliable Internet filtering system is in place.
- Develop and implement an Internet Security Policy that includes, by way of example, the requirements prescribed in this policy.
**Principal** will:
- Schedule continuing professional development to keep teachers aware of the most
recent Internet safety developments.
- Periodically review the School’s technology infrastructure with appropriate technology staff, make improvements as needed.
**Teachers, librarians and other staff members** will, at a minimum:
- Educate students not to open e-mail or attachments from unknown sources.
- Ensure there is an academic purpose before allowing students to go online
(students should not be allowed to surf the Internet without a specific purpose).
- Educate students on the types of information that are safe to share with others
online, and information that should never be shared as it could put them at risk.
- Teach students to recognize the various forms of cyber-bullying and know what
steps to take if confronted with that behavior.
- Inform students of all aspects of the School’s Internet Policy.