ICT FACILITIES - ACCEPTABLE USE POLICY FOR STUDENTS

PURPOSE

ICT facilities are used extensively in schools for teaching and learning. The purpose of an acceptable use policy is to clearly outline the expected behaviour of students using these facilities.

The definition of ICT facilities for the purpose of this document includes the following:

- All computers, including desktop PCs, laptops, and netbooks
- All peripheral devices, such as mice, keyboards, screens, cables, printers, scanners, digital cameras, data projectors, LCD panels
- All software packages and operating systems
- All connected services including the Internet, the school’s Local Area Network (LAN) and Wireless Local Area Network (WLAN), the Intranet and all network storage
- Computer suites, classrooms and learning areas where ICT is being used

Ensuring that this policy has been read and clearly understood is vital in ensuring that students are able to use the ICT facilities productively and safely.

This policy has been developed in accordance with the DECS Standards document:


RESPONSIBILITIES

It is the responsibility of the student to:

- Ensure that their log in credentials (username and password) remain confidential
- Change their password if they suspect it has been learned by others
- Use the ICT facilities for educational purposes only
- Report any damaged or malfunctioning equipment to relevant staff
- Report any unacceptable use of ICT facilities by other students
BEHAVIOUR

It is unacceptable for a student to:

- Log on to a computer or the internet using another student or staff member’s credentials
- Attempt to bypass the school’s content filtering system
- Modify any system settings while logged on to a school computer including:
  - Disabling the firewall or anti-virus software
  - Changing internet proxy settings
  - Installing software
- View, send, or share any material that may be deemed inappropriate, for example:
  - Pornography or sexually suggestive material
  - Offensive, hateful, violent, discriminatory material
  - Unsolicited emails (Spam) or intentionally sending viruses or other malicious software
- Intentionally cause damage to any ICT facilities, or behave in a way which could cause accidental physical damage
- Plagiarise the intellectual property of other students, or publish any copyrighted material

SAFETY

Students will tell a teacher immediately if:

- They receive any emails, transmissions, or messages containing:
  - Material of an abusive or bullying nature
  - Indecent or unreasonable requests (such as requesting personal information)
  - Defamatory or untrue information relating to themselves or others
- They suspect another student of using their log in credentials to harass or bully others

MONITORING

The school’s network and internet are monitored at all times and inappropriate behaviour will be reported by technical support staff to school leaders.

CONSEQUENCES

Any student found to be behaving inappropriately will be disciplined according to the school’s Behaviour Management policy