4.7 Internet acceptable use

Introduction

This Acceptable Use Policy (AUP) for the internet is to ensure that students and employees will benefit from learning opportunities offered by the school's internet resources in a safe and effective manner. It applies to all students for the full duration of their studies in this school and to all those employed by the school.

Internet use and access is considered a school resource and privilege. Therefore, if this AUP is not adhered to this privilege will be withdrawn and appropriate sanctions – set out below – will be imposed.

This policy is framed in the context of St. Michael's being a health promoting school. Consequently, the school is one that seeks to promote healthy lifestyles for all in a safe, supportive and non-threatening environment. The policy is also mindful of the need to bring the key components of the school's mission statement.

Legislation

There is no specific legislation governing internet safety at school level. This is complicated by the fact that the internet functions in a global context whereas the law functions in a localised one. The following pieces of legislation, however, have relevance to internet safety:

- The Child Trafficking and Pornography Act, 1998

This Act legislates against any one who knowingly produces, prints, publishes, distributes, exports, imports, shows, possesses or sells child pornography.

- The Interception of Postal Packets and Telecommunications Messages Regulation Act, 1993

This Act stipulates that telecommunication messages can be intercepted for the purpose of an investigation of a serious offence.

- The Video Recordings Act, 1989

This prohibits the distribution of videos which contain obscene or indecent material which may lead to the depravation or corruption of the viewer.

- The Data Protection (Amendment) Act, 2003

This Act was passed to deal with privacy issues arising from the increasing amount of information kept on computer about individuals.

A. Strategy in relation to the school's internet resources

General

- Students can only use the school's internet resources when supervised by a teacher.
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material.
- Computer teachers will regularly monitor students' usage of the school's internet

resources.

- Students, parents and teachers will be provided with information in the area of internet safety.
- Uploading and downloading of non-approved software will not be permitted.
- Virus protection software will be used and updated on a regular basis.
- The use of, memory sticks or CD-ROMs in school requires a computer teacher's permission.
- When using the school's internet resources, no one – staff or student - will undertake any actions that may bring the school into disrepute.
- It will be the responsibility of the school's ICT Co-ordinator to ensure that all IT equipment is properly protected by anti-virus software and firewall system. The nature and extent of the firewall will be kept under ongoing review by the ICT Co-ordinator and Principal. Child protection will be the foremost principle underpinning such review.

World Wide Web

- No one will visit internet sites from the school's internet resources that contain obscene, illegal, hateful or otherwise objectionable materials.
- Students will use the internet for educational purposes only.
- Students/employees must be aware of and comply with copyright issues relating to online learning.
- Students will never disclose or publicise personal information.
- Downloading by student of materials or images not relevant to their studies is in direct breach of the school's acceptable use policy
- Students are to be aware that usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.

Email

- No one using the school's internet resources will send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person.
- Students must not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.
- Students will never use email to arrange a face-to-face meeting with someone.
- Students will note that sending and receiving email attachments is subject to permission from their teacher.

Internet chat

- Students will only have access to chat rooms, discussion forums or other electronic communication forums on the school's internet resources that have been approved by the school. These forums will only be used for educational purposes and will always be supervised.
- Usernames will be used to avoid disclosure of identity.
- Face-to-face meetings with someone organised via internet chat will be forbidden.

School website

- Students will be given the opportunity to publish projects, artwork or school work on the world wide web. The website will be regularly checked to ensure that there is not content that compromises the safety of students or staff
- The publication of student work will be co-ordinated by a teacher.
- Students' work will appear in an educational context on web pages with a copyright notice prohibiting the copying of such work without express written permission.
- Photographs, audio and visual clips will focus on group activities and not on individual students. Video clips will be password protected.
- Personal student information including home address and contact details will be omitted from school web pages.
- Students will continue to own the copyright on any work published.

B. Strategy in relation to student personal devices (phones, i-pod, i-pad etc.)

Students using their own technology (with or without internet access) in school in the following ways will be in direct breach of the school's acceptable use policy:

- leaving a device turned on or using it in class
- sending nuisance text messages via phone or social networks the unauthorized taking of images with a mobile phone camera, still or moving
- accessing obscene, illegal, hateful or otherwise objectionable materials

B. Sanctions

Misuse of technology as set out in A. and B. above may result in disciplinary action, including written warnings, withdrawal of access privileges, detention and, in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities.

D. Role of parents

It is expected that, as primary educators and protectors of their daughters, parents will inform themselves of child protection matters relating to internet safety and impress upon their daughters the need for absolute compliance with the terms of the above policy and procedures.

E. Review

This policy will be reviewed on a regular basis because of the changing nature of the subject matter.