St. Paul's College, Raheny, Dublin

Computer System - Acceptable Use Policy Background to the Policy

The aim of this policy is to ensure that students will benefit from learning opportunities offered by the school's computer and Internet resources in a safe and effective manner. In drafting this policy, access to the school's computer system and associated Internet use is considered a valuable school resource and privilege.

School's Strategy

The school employs a number of strategies in order to maximise learning opportunities and reduce the risks associated with the Internet. Within these strategies, a number of unacceptable uses are defined. These strategies are as follows:

Computer System

- Students can only use the computer system for educational and career development reasons.
- Students may not use the computer system to provide or purchase goods or services for personal gain.
- Every student is supplied with their own account and username. Users must log onto the system with this username and their own password. Students must not disclose this password to other students. A sanction will be imposed if students forget this password or disclose this password to other students
- To protect the computer system, virus protection software is used and updated on a regular basis. Consequently, the use of personal memory sticks, CD-ROMs or DVDs in the school's computer network requires a teacher's permission and all such disks must be virus scanned before usage.
- Students should be aware that St. Paul's College is not responsible for the loss of data. There will be no warranties of any kind, whether expressed or implied, for the network services offered by the school. These damages include loss of data as a result of delays, ondeliveries, or service interruptions caused by the system or your errors or omissions for example DCG projects and online ECDL exams. Use of any information obtained via the network is at your own risk

Use of the Internet

- Students must use the Internet for educational purposes only.
- Internet classes are always supervised by a teacher
- Filtering software (Fortinet) is used to minimise the risk of exposure to inappropriate material.
- Any student's internet usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.

-

- Students will be made aware of Internet Safety as an integral part of the First Year Programme.
- Students are not permitted to upload or download non-approved software.

  Students must observe good "netiquette" (i.e., etiquette on the Internet) at all times and must not undertake any actions that bring the school into disrepute.
- Students may not post false or defamatory information about a person or organisation.

World Wide Web

- Students must be familiar with the many copyright issues involved with the Internet such as software piracy, copyright infringement, music and videodownloads and others. If in doubt regarding a copyright issue, a student must contact the supervising teacher.
- Students can only access discussion forums or other electronic communication forums that have been approved by the school. Such discussion forums and other electronic communication forums are only used for educational purposes and are always supervised.
- Students must not visit Internet sites that contain obscene, illegal, offensive or otherwise objectionable materials. If inappropriate sites are mistakenly accessed, students must report this immediately to your supervising teacher.Students are reminded that accessing websites is for educational purposes only
- Students must never disclose or publicise their own or other people's personal information (such as addresses including internet addresses, telephone numbers, photographs or pictures) and usernames must be used to avoid disclosure of identity.
- Face-to-face meetings with someone contacted using Internet discussion forums or through emails are unsafe and therefore forbidden.

Email

- Students must use approved class email accounts under supervision by or permission from a teacher. The school may inspect personal email at any time and without notice.
- Students must not use disrespectful language in their emails. Any material that is illegal, obscene, and defamatory or material that is intended to annoy, harass or intimidate another person may not be sent or received.
- Students can only send and receive email attachments subject to permission from their teacher. Similarly, attachments can only be opened, once they are virus scanned and with the permission of the teacher.
- Emails that you have received which are inappropriate or make you feel uncomfortable must be reported immediately to the supervising teacher. Similarly, if such material is mistakenly accessed, it must be also reported immediately.

School Website

- Students are encouraged to publish projects, artwork or school work on the school website. The publication of student work will be co-ordinated by a teacher.
- Students' work which appears in an educational context on Web pages will appear with a copyright notice prohibiting the copying of such work without express written permission

-

- Digital photographs, audio or video clips of individual students are not published on the school website. Instead photographs, audio and video clips focus on group activities. Video clips may be password protected.
- Personal Student information including home address and contact details are omitted from school web pages.
- Students continue to own the copyright on any work published.
  Parents/Guardians are requested to inform the school in writing if they have any objection to the publication of work etc.

Virtual Learning Environments

The school is involved in a pilot moodle project, hosted and managed by Dundalk IT. This is a webbased interface that assists learning and teaching by providing and integrating online resources and tools and is available both in school and at home. In order to use this platform:

- Students must not access, distribute or place on their moodle page any material that is illegal, offensive or otherwise objectionable
- Students must be aware that text, images and other information created by third parties will be subject to the laws of copyright, and that includes material found elsewhere on the internet
- E-mail, messaging or chat must not be used to harass or intimidate other people, whose views and beliefs, must be respected at all times. (Please refer to schools' anti-bullying policy)
- Students should be aware that site administrators and teachers can directly access students files and records are kept of all students activities

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

Students and parents can familiarise themselves with the following legislation which is available online:

- Data Protection (Amendment Act) 2003
- The Child Trafficking and Pornography Act, 1998
      This Act legislates against anyone who knowingly produces, prints, publishes, distributes, exports, imports, shows, possesses or sells child pornography.

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

-

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

- The Video Recordings Act, 1989

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

The Data Protection Act, 1988

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

-

Support Structures

There are key support structures and organizations that deal with illegal material or the harmful use of the Internet. Some useful websites include:

- www.webwise.ie
- www.ncte.ie
- www.skoool.ie

Sanctions

If there is misuse of the Internet or if the school's acceptable user policy is not adhered to, then the privilege of computer access will be withdrawn and appropriate sanctions in accordance with the school's Code of Behaviour will be imposed. Such sanctions may include written warnings, withdrawal of access privileges and, in extreme cases, the student's future in school will be considered. The school also reserves the right to report any illegal activities to the appropriate authorities.

The school accepts that you and have read the Acceptable Use Policy and grant permission for your son to access the Internet. This is based on the understanding that Internet access is designed for educational purposes.   It is also on the understanding that every reasonable precaution has been taken by the school to provide for online safety but the school cannot be held responsible if students access unsuitable websites.

The school also accepts that your son too has read and agrees to follow the school's Acceptable Use Policy on the use of the Internet and that he agrees to use the Internet in a responsible way and obey all the rules explained to her by the school.