St Paul's Secondary School

Care - Inclusion - Respect

INFORMATION & COMMUNICATION POLICY

Ratified: 10 March 2011

To be reviewed: January 2021

ICT POLICY

School Name: St. Paul's Secondary School

Address: Greenhills, Dublin 12

St. Paul's ICT Policy has been formulated in conjunction with St. Paul's Acceptable Use Policy. The aim of this ICT Policy is to ensure that pupils and teachers will benefit from the teaching and learning opportunities offered by the school's computer resources in an effective manner. Computer use and access is considered a school resource and privilege. Therefore, if the school ICT policy is not adhered to this privilege will be withdrawn and appropriate sanctions will be imposed.

It is envisaged that the ICT policy will be reviewed annually. Before signing, the ICT Policy it should be read carefully to ensure that the conditions of use are understood and accepted.

Introduction

Teaching and learning is currently undergoing a transformation as schools strive to incorporate e-Learning (technology enhanced learning) into their existing practices. This new "blended learning" involves the use of ICT by a much larger number of teachers than previously. St. Paul's Secondary School aims to use ICT to enrich and enhance the learning experience of students. Available finance for hardware, software and technical support as well as the availability of training for teachers control the pace and extent of the move towards blended learning. St. Paul's has always acknowledged the importance of encouraging students to use ICT in a variety of situations and contexts to prepare them for the digital world in which they live. For this reason, students have formal I.T. classes introducing them to commonly used software applications and good computer practice.

This policy is being put in place to strive to keep computers and other technological resources in optimal working condition. This is vital if ICT is to

contribute to the learning experience of students. In addition to the student computer rooms, the policy applies to e-learning equipment in individual classrooms and equipment in offices and the staffroom. This policy is applicable to any student, member of staff or visitor who uses any of the school's technological resources. These will be referred to as "the users" throughout this document.

Policy Statement

St. Paul's computer resources are the property of the Board of Management and may only be used for legitimate educational purposes. Users are permitted access to ICT to assist them in their work and/or to enhance teaching and learning in class. Everyone using St. Paul's ICT resources has a responsibility to give full and active support to this policy.

Privacy

The computer resources and the computer accounts given to users are to assist them in the performance of their work. Users do not have privacy, nor should they have an expectation of privacy, in anything they create, store, send or receive on the computer systems. St Paul's Secondary School has the right, but not the duty, to monitor any and all aspects of its computer systems. Users are hereby notified that St. Paul's may use human or automated means to monitor use of its computer resources.

Prohibited Activities

Users encountering material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating or defamatory should report the incident to Management.

St. Paul's computer resources may not be used for dissemination or storage of commercial or personal advertisements, solicitations or promotions. Neither are the school's computer resources to be used for the storage of destructive programs (such as viruses or self-replicating code), political material or any other unauthorised use.

Students may not use St. Paul's computer resources and/or Internet connection to play or download games and other entertainment software, including screen savers. Non-student users may download games and entertainment software only if these games and software enhance teaching and learning in the school.

Users may not deliberately act in a way that wastes St Paul's computer resources or unfairly monopolises resources to the exclusion of others. This includes printing unnecessary copies of documents or otherwise creating network traffic. It also includes booking the computer room for the same period of every week of a term or school year.

Users may not introduce software onto any school computer or modify existing software without the express permission and involvement of the ICT co-ordinator.

Users may not illegally copy software or applications protected under copyright law to or from school computers or make that material available to others for copying in school. Users are responsible for complying with copyright law and the terms of software licences. Users may not agree to a licence or download any material for which a registration fee is required.

St. Paul's is not responsible for material viewed or downloaded by users from the Internet. Users accessing the Internet do so in accordance with the terms of St. Paul's Acceptable Use Policy.

Passwords

Users are responsible for safeguarding their passwords for access to the computer resources. Each classroom laptop has a unique password, which must not be revealed to students. Staff and students have usernames and passwords which should not be printed, stored online or given to anyone else. Users are responsible for all transactions made using their user account. If a user suspects that the security of an account has been compromised, this should be reported to the ICT co-ordinator.

Use of passwords to gain access to the computer system does not imply that users have an expectation of privacy for the material that they create, send or receive on the school's computer systems.

Security

Attempting to breach or circumvent security or permitting another person to do is prohibited. The express permission and active participation of the ICT co-ordinator must be sought before any device is connected to St. Paul's networks. This includes but is not limited to servers, workstations, printers, modems and other network devices.

Users may not alter or copy a file belonging to another user without first obtaining permission from the owner of the file. Users may not use the computer system to pry into the affairs of others by unnecessarily reviewing their files.

Each user is responsible for ensuring that the use of outside computers and networks such as the Internet does not compromise the security of St. Paul's computer resources. This duty includes taking reasonable precautions to prevent intruders accessing St. Paul's network without authorisation and to prevent the introduction and spread of viruses.

Users have the responsibility to log-off after each use of a password protected computer resource to prevent others from accessing resources or access privileges.

Viruses and Malware

Viruses, trojans, spyware, malware and any type of malicious software can cause substantial damage to computer systems. Each user is responsible for taking reasonable precautions to ensure that he or she does not introduce any such malware into St. Paul's computers and/or networks. To ensure this, all material opened from an external storage device (including USB keys, mobile hard disks, optical and magnetic storage devices) as well as all material downloaded from the internet and email attachments must be scanned using the security software on the computer or network where it is being opened. Users should understand that their home computers and laptops might contain viruses. Students should not be encouraged to bring in work on USB keys. It is preferable that any such work would be emailed to a school email address with the work included in the body of the email and not as an email attachment. Alternatively, the use of cloud space with files being scanned before they are opened is preferable to the use of USB keys. If a teacher requests a student to bring in work on a USB key it is essential

that the teacher takes the USB key and scans it before it is used on a school computer. ICT teachers cannot allow students to use USB keys for a different subject without written confirmation from another teacher to say that the key has been scanned since it was last used on the student's home computer.

Users with knowledge of or suspecting the introduction of a virus into St. Paul's computers or networks should notify the ICT co-ordinator as soon as possible. Users should be aware of the name of the security software on any computer that they use in school. Messages about viruses, trojans etc from these applications should be taken seriously. Users should be aware of the existence of scareware and not download or enable any software to remove malware unless it is coming from the official security provider on the machine.

Responsibility

It is the responsibility of every user to ensure full compliance with the procedures and guidelines laid down in this policy. Failure to do so may result in disciplinary procedures.

Misunderstanding of the provisions of the policy will not be considered to be an adequate response as to why a prohibited activity was performed.

If a user is uncertain about whether an activity is admissible under this policy or the AUP they should contact the ICT Co-ordinator for clarification.

This policy was ratified by the Board of Management on: 10th March 2011