St Olave's Grammar School

STUDENT ACCEPTABLE USE OF NETWORK POLICY

1.0 Overview

The intention for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to St Olave's Grammar School's established culture of openness, trust and integrity. The School seeks to protect its staff, students, and the Governing Body from illegal or damaging actions by individuals, either knowingly or unknowingly.

The School network related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, internet browsing and FTP are the property of the School. These systems are to be used primarily for School related purposes in the course of normal day-to-day activities. The use of the School network related facilities is permitted for occasional personal use; for example, non-school related use of email and the internet but these activities are also subject to this acceptable use policy.

It is the responsibility of every School computer user to be familiar with these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at the School. These rules are in place to protect the student and the School. Inappropriate use exposes the School to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to ALL student users of the School network. This policy applies to all computer equipment that is owned or leased by the School, including the use of privately owned equipment which is used to connect to the school network[1] and/or to the internet via the school's wireless 'hotspot'.

[1] Permission must be sought from the IT manager to use privately owned equipment on the school network.

4.0 Policy

4.1 General Use and Ownership

1. While the School desires to provide a reasonable level of privacy, students should be aware that the data they create on the School systems remains the property of the School. Because of the need to protect the network assets, the confidentiality of information stored on any network device belonging to the School cannot be guaranteed.
2. Students are responsible for exercising good judgment regarding the reasonableness of personal use, if there is any uncertainty, students should consult the I.T. manager.
3. For security, network maintenance and child protection purposes, authorized individuals within the School will monitor equipment, systems and network traffic using specialist software.

4.2 Security and Proprietary Information

1. All pupil and staff details[2], including photographs, are considered to be confidential and should not be disclosed to third parties, without the prior agreement of the Headmaster or Deputy Headmaster.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. The school system will automatically prompt students to change their user passwords every six weeks before allowing them to log on. Personal laptops should be secured with a password-protected screensaver or by logging-off when the laptop is unattended. Students are allowed to use their own laptop via the wireless 'hotspot', which use the school web-filtering software.
3. Postings by students from a School email address should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the School.
4. Students must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses. If in doubt seek the advice of the I.T. manager.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Under no circumstances is a student of the School authorized to engage in any activity that is illegal under national or international law while utilizing School owned resources or accessing school systems with private equipment.

The lists below are by no means exhaustive but attempt to provide a framework for activities that fall into the category of unacceptable use.

[2] Including personal addresses, telephone/fax numbers or e-mail addresses of any adult or student at the school.

System and Network Activities

The following activities are **strictly prohibited**, with **NO** exceptions:

1. Unauthorized copying of copyrighted material including digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the School or the end user does not have an active licence is strictly prohibited.

2. Introduction of malicious programs into the network or server (e.g., viruses)

3. Revealing your user password to others or allowing use of your account by others.

4. Using the School computing assets to actively engage in the viewing, creation or distribution of any sounds, messages or other material which are obscene, harassing, racist, inflammatory, malicious, fraudulent or libellous, and which would otherwise damage the reputation of the School.

5. Indecent images of children under the age of 18 are illegal. Making an indecent image of a child is a Criminal Offence carrying a maximum sentence of 10 years imprisonment. The term “make” includes downloading images from the Internet and storing or printing them out.

6. Accessing, or attempting to access data of which the user is not an intended recipient or logging into another staff or pupil account that the student is not expressly authorized to access. Circumventing user authentication or security of any work-station or user account.

7. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, the work of others, or result in the person receiving them losing their work or system access.

8. Providing information about, or lists of, users to parties outside the School.

Electronic Communications Activities (Texting, E-mail, Social Networking, Facebook, Twitter, etc.)

1. Sending unsolicited messages, regarding the School to individuals who did not specifically request such material.
2. Any form of harassment whether through language, image, frequency, or size of messages.
3. Unauthorized use or forging of communications, such as email header information or digital signatures.
4. Solicitation of communications with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", or other "pyramid" schemes of any type.
6. You must inform the I.T. manager immediately if you receive an email communication that you believe advertises a website containing indecent images of children.

5.0 Enforcement

In the event of a violation of this policy:

- Students will lose access to the School network related facilities on a temporary or permanent basis.
- A letter will be sent to your parents/guardians informing them of the nature and breach of rules
- Any other action decided by the Headmaster
- When applicable, police or local authorities may be involved.

STUDENT

I agree to comply with this 'Acceptable Use Policy'. I will use the network facilities in a responsible way and observe all the restrictions explained to me by members of staff as well as those listed above.

Pupil Signature_____ Date_____

PARENT/GUARDIAN

As the parent or legal guardian of the student signing above, I grant permission for my son or daughter to access the school network resources. I understand that students will be held accountable for their own actions. I also understand that some materials on the Internet may be objectionable and I accept responsibility for setting standards for my son or daughter to follow when selecting, sharing and exploring information and media.

Parent Signature_____ Date_____

Name of Student_____ Form_____