ST. JOSEPH'S
CATHOLIC COLLEGE

Acceptable Use Policy 2014

Reviewed July 2011

St. Joseph's Catholic College Technology Resources Policy

St. Joseph's Catholic College provides technology for use by all its stakeholders, offering access to a vast range of valuable information for use in education. It is also an enormous addition to the information base held in the Independent Learning Centre (ILC) that helps students to prepare for life in today's world.

Because this technology is provided and maintained for the benefit and enjoyment of all members of the College community, there is a responsibility for everyone to take care of the equipment and protect these resources for use by future year groups. As such, everyone in the College is expected to adhere to the acceptable use policy as outlined below.

The College reserves the right to examine or delete any files that may be held on its computer system and to monitor the network; this includes internet sites and the exchange of e-mails. It is important that all members of the College respect the rules for computer and internet security as outlined below.

Due to the demands of some academic courses, there may be an exemption from some of the rules for very short periods of time during lessons; this is when students will be required to perform certain tasks as part of their lessons (e.g. changing settings may be part of a particular ICT course). In these special cases, the teacher will give specific permission.

Key terms:

Technology = PC's, printers, external devices, mobile phones, PDA's, USB devices, Bluetooth, mp3 etc

Users = anyone who uses the resources (students, staff, parents, governors, community etc)

Exchange information = any technology device used e.g. Internet, email, Bluetooth, USB device etc

Technologies Rules

1. All internet use should be for educational purposes and comply with the South West Grid for Learning acceptable user policy.
2. Users may not install or attempt to install programs of any type on a machine, or store programs in the computers.
3. Users must not damage, disable, steal or otherwise harm the operation of the equipment, or intentionally waste limited resources.
4. Users will not use the network for commercial purposes, personal financial gain, gambling, political issues and advertising.
5. Users must not disclose their passwords to others or use others user passwords.

6. Making use of technologies must be applied in a way that does not harm, harass, offend or insult others.
7. Users are expected to respect and not attempt to bypass or alter security settings.
8. Users must not access, copy, remove or otherwise alter other user's work.
9. Users must not alter computer settings.
10. Users may apply personal external devices such as mobile phones, PDA's, USB devices, mp3, mp4 etc when planned for educational purposes and their teacher gives permission. Inappropriate use will result in equipment being confiscated in line with College policy.
11. Any faults with equipment MUST be reported to the teacher and users should not make attempt at repairs.
12. Users must not disclose or share personal information of themselves or others on-line.
13. Activity that threatens the integrity of the College ICT systems, or that attacks or corrupts other systems, is forbidden.
14. Users must not engage in chat/social networking/instant messaging activities over the Internet unless authorised to do so by a teacher. Such activities take up valuable resources which could be used by others to benefit their studies and can lead to unwelcome material being brought into the College.
15. Users must not access the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are inappropriate, unlawful, or that may cause harm or distress to others.
16. Users are responsible for exchanging information via digital communication and therefore the same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded.
17. Posting anonymous messages and forwarding chain letters is forbidden.
18. Users are expected to respect the work and ownership rights of people both inside and outside the College. This includes abiding by laws relating to technologies e.g. copyright laws.

Sanctions

1. *Violation of these rules will result in disciplinary action in line with College behaviour policy.*
2. *Where clear laws have been broken, appropriate external agencies may be contacted e.g. SWGfL, Police.*

By agreeing to the above <u>YOU AGREE</u> to use the College technology facilities in a responsible manner.

Pupil Name …… Signed …….

Tutor group …… Date …….

Parent/Guardian signature ……..

Reviewed July 2011

ICT CODE OF CONDUCT

The College endorses 'fit for purpose' use of Information, Communication and Technologies resources. This means that during a lesson, students must be using programmes, text and images that are appropriate and 'on task'. This fit for purpose use of ICT extends outside the College when and if it impacts on other St. Joseph's students.

If you cannot show the adult in the room what you are doing or using, then the chances are that it's not 'fit for purpose'.

As you are aware, the College upholds Gospel values, which shows our intention to be more than just a mirror on society. Our intention is to be better than this.

The following sanctions are our commitment to being better.

Stage 1

- Accessing email or the internet without permission will result in a C1 initially.
- Attempting to access websites not related to learning will result in a C1 initially.
- Removing or copying other students work will result in a C2 detention.

Stage 2

- Accessing or file sharing inappropriate sites, e.g. pornographic, racist materials.
- Cyber bullying of any sort.

The College considers these to be sufficiently serious for sanctions to be put in place immediately. These will include access to the internet and email being temporarily removed for two weeks.

Repeat offenders will lose access to the internet and email for up to four weeks. A parent meeting will be held and students will spend time in seclusion.

Stage 3

- Students who continue to flout the system will meet with the Headteacher and further sanctions will be considered which may include permanent removal of ICT privileges at St. Joseph's Catholic College.

Legislation relating to Technologies

Reviewed July 2011

The user must comply with all relevant legislation and legal precedent, including the provisions of the following Acts of Parliament, or any re-enactment thereof:

- Copyright, Designs and Patents Act 1988;
- Malicious Communications Act 1988;
- Computer Misuse Act 1990;
- Criminal Justice and Public Order Act 1994;
- Trade Marks Act 1994;
- Data Protection Act 1998;
- Human Rights Act 1998;
- Regulation of Investigatory Powers Act 2000;
- Freedom of Information Act 2000;
- Communications Act 2003.

See below for a summary of the main points.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in any work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Malicious Communications Act 1988
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Computer Misuse Act 1990
This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:-

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or

- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Data Protection Act 1998
This protects the rights and privacy of an individuals data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discreet subject area within the law. It is a type of "higher law", affecting all other laws. In the College context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom expression
- Freedom of assembly
- Prohibition of discrimination
- The right to educate

These rights are not absolute. The College is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to ascertain whether the communication is business or personal
- Protect or support help line staff.
- The College reserves the right to monitor its systems and communications in line with its rights under this act.