St Joseph's College
Borrisoleigh,
Thurles, Co. Tipperary.
Phone (0504)51215

ICT & Social Media Acceptable Use Policy

St Joseph's College aims to ensure that students will benefit from learning opportunities offered by the access to Information & Communication Technology (ICT) & the school's ICT resources, in a safe and effective manner. ICT use and access is considered a school resource and privilege. Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions, as outlined in the AUP, will be imposed.

School's Strategy

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

Aims in use of ICT

- Adhere to the Current Digital Learning Plan
- That every student develops the necessary ICT skills and understanding to make their contribution to the economy and the society of their future.
- That students' learning in all areas is enhanced and enriched.
- That the range of teaching strategies is broadened, to increase effective teaching and in particular providing better access to the curriculum for pupils with Special Educational Needs.
- That the students take more responsibility for their own learning.
- That the students develop a positive attitude towards ICT.
- That students learn the basics computer applications
- To allow access to a wealth of electronic resources on the Internet.
- To use all available hardware and software resources to ensure the effective and efficient administration of the school.
- That staff develop and maintain the necessary ICT skills to make a contribution to the development of the school academically and administratively.

St Joseph's College provides ICT for staff and students. This policy outlines the guidelines and behaviours that our students and staff are expected to follow when using school technologies, or when using personally owned devices, on school premises, at home using 365 portal or on school organised activities. Student and staff are expected to understand the risks, act responsibly and be accountable for their actions when using ICT.

Technologies Available

St Joseph's College may provide students and staff with Internet access (WiFi), desktop computers, digital imaging equipment, laptop, tablet or mobile devices, video conferencing capabilities, virtual learning environments (VLEs), online collaboration capabilities, online discussion forums, email, various appropriate educational software and more.

As new technologies emerge the school may offer these also.

The policy is intended to cover all technologies, online and offline, which may be used in the school, not just those mentioned.

Legislation

There is as of now 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 localized one.

The following legislation does have relevance to internet safety:

- Child Protection Procedures for Primary and Post-Primary School 2017
- Children First 2015
- The Child Trafficking and Pornography Act, 1998
- The Interception of Postal Packets and Telecommunications Messages Regulations Act 1993
- The Video Recordings Act 1989
- The data Protection (Amended) Act 2003
- The Teaching Council Act 2001

The ICT Network in St Joseph's College

The computer network is intended for educational purposes, thus:

- All activity over the network may be monitored and retained.
- Access to online content via the network is restricted in accordance with our policies and the DES through its agency, the PDST Technology in Education.
- Users are expected to respect that the web filter is a safety precaution and should not try to circumvent it when browsing the Web. If a site is blocked and a student believes it shouldn't, the student can ask the teacher to submit the site for review. This is done via the PDST Technology in Education filtering service, 'BrightCloud'
- Students are expected to follow the same rules for good behaviour and respectful conduct online as offline – these rules can be found in the Code of Behaviour and Anti-Bullying Policy.
- An Acceptable Use IT agreement form is in every student's diary and must be signed by both student and parent/guardian. Failure to do so may result in suspension of IT use until agreement with AUP. (See Appendix 1)
- Office 365 is available for all staff and students. Student use Office 365 to access their email accounts and submit work to teachers through the 'Teams app'.
- Misuse of the school resources may result in disciplinary action.
- The school makes a reasonable effort to ensure students' safety and security online, but will not be held accountable for any harm or damages that result from the misuse of school technologies.
- Students are expected to alert their teacher immediately of any concerns for safety or security.
- Any concerns reported by a student or noticed by staff must be reported to the ICT Coordinator immediately.
- Changes to the web filter level. Or temporary suspension of web filtering for staff training or adult education, must be agreed and authorized by the Principal and the ICT Coordinator.
- Staff should use a PC that has unrestricted or low-level web filtering with caution and ensure that no obscene, illegal, hateful or otherwise objectionable materials are acceded, downloaded or displayed.

Security

The availability and integrity of the school network is of paramount importance, thus

- Attempting to breach or circumvent security, or permitting another person to do so, is prohibited. The express permission and active participation of the ICT Coordinator must be sought before any device is connected to St Joseph's College networks. This includes but is not limited to servers, workstations, printers, modems and other network devices.
- Users may not alter or copy 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 Joseph's College's computer resources. This duty includes taking reasonable precautions to prevent intruders and spread of viruses.
- The school reserves the right to read all memory sticks and storage devices, and to check them for 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.

Privacy and Passwords

The computer resources and the computer and email accounts given to users, are to assist them in the performance of their work. Users do not have privacy, nor should they have any expectation of privacy in anything they create, store, send or receive on the computer system.

- St Joseph's College has the right but not the duty to monitor any and all aspects of its computer systems and may use human or automated means to monitor use of its computer resources. St Joseph's may, as a requirement of system maintenance, delete files that re determined to be non-essential.
- Staff and students have usernames and passwords for access to electronic resources and email facilities, which should not be given to anyone else. Users are responsible for safeguarding their passwords and are responsible for all actions made using their user account. If a user suspects that the security of their account has been compromised they should contact the ICT Coordinator immediately.
- Use of passwords to gain access to the computer system does not imply that users have an expectation of privacy for the material they may create, send, receive on the school's computer system.

Viruses & Malware

Students are expected to take reasonable safeguards against the transmission of security threats over the school network.

- This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin.
- If a student thinks that a website does not look right, the teacher must be informed.
- If a student believes a computer or mobile device being used might be infected with a virus, the teacher must be alerted immediately. He must not attempt to remove the virus himself or download any programs to help remove the virus.
- Students should not download, or attempt to download, or run, .exe programs over the school network or onto school resources. Students may be able to download other file types, such as images or videos. Such files should only be downloaded from reputable sites, and only for educational purposes.

Netiquette

Netiquette may be defined as appropriate social behaviour over computer networks and in particular in the online environment. To this end:

● Students should always use the Internet, network resources, and online sites in a courteous and respectful manner

● No-one will undertake any actions that may bring the school into disrepute.

● Students and staff should not violate the copyrights of material.

● Students should also recognize that among the valuable content online is unverified, incorrect, or inappropriate content. Students should use trusted sources when conducting research.

● Students should not to post anything online that they wouldn't want parents, teachers, or future colleges or employers to see. Once something is online, it is fully available and cannot be removed; ownership of the information may have been relinquished, and it can sometimes be shared and spread in ways never intended.

● Students may not post any work, images, sound or movie recordings into public forum, without the express permission of the teacher. St Joseph's College email, Social Media, and online collaboration recognises that online collaboration is essential to education and may provide students with access to a variety of online tools that allow communication, sharing, and messaging among students and staff. Eg Office 365 'Teams'

● St Joseph's College have provided students and staff with email accounts for the purpose of school-related communication. Availability and use is restricted based on school policies. Email accounts should be used with care. Email usage may be monitored and archived.

● Users are expected to communicate with the same appropriate, safe, mindful and courteous conduct online as offline.

● Online communication with teachers may only be made using the @stjosephscollege.ie email addresses.

● Use of school networks, email accounts, servers and/or equipment for financial or commercial gain, or for illegal activity, is prohibited.

● Staff should not respond to any non-educational contact made by a student: friend request, text message, email using any non-school address or regarding any non-educational matter. Any concern should be raised with the Designated Child Protection Officer St Joseph's College. St Joseph's College may provide students with mobile computers, digital recorders, cameras or other devices to promote learning both inside and outside of the school.

● Students should abide by the same Responsible-use policies, when using school devices off the school network, as on the school network.

● Students are expected to treat these devices with respect. They should report any loss, damage, or malfunction to their teacher staff immediately.

● Use of school-issued devices will be monitored.

Mobile devices in the possession of St Joseph's College students

Students may use personally-owned devices (e.g. laptops, tablet-computers, digital-cameras, and smart-phones) for educational purposes, if explicitly permitted by their classroom teacher.

● Appropriate online behaviour and adherence to the Responsible Use Policy should always be used.

● St Joseph's College do not accept responsibility for the loss of or damage to students' own technologies.

● It is a user's responsibility to keep devices safe and secure

● Students must use and position any device in the manner as directed by staff.

● St Joseph's College reserves the right to monitor the use, and inspect the contents, of any mobile device used in school. St Joseph's College reserves the right to confiscate devices to ensure compliance with this Responsible Use Policy; devices must be surrendered immediately, without alteration, upon request by any member of staff.

● 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 Responsible Use Policy, if:

1. leaving a device turned on or using it in class, unless explicitly permitted by their classroom teacher,
2. sending nuisance messages via mobile or social networks,

3. the unauthorised taking of images, still or moving, and the unauthorised recording of sound, with any device.
4. accessing, sending, receiving, uploading, downloading, distributing, or storing offensive, threatening, hateful, obscene, sexually explicit, illegal or otherwise objectionable materials.

● Students must not use devices in school corridors, on journeys to and from school, or outside school buildings, unless with a teacher's permission.

● Photographs, audio and visual clips will focus on group activities and not on individual students. Personal student information including home address and contact details will be omitted from school web pages.

Plagiarism

Students should not plagiarise content (copy or use as your own without citing the original creator), including words or images, from the Internet.

● Students should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Personal Safety

Students are expected to take responsibility for their personal safety and should never act in such a way that may compromise their or another's safety.

● If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the immediate attention of a teacher if you are at school; and a parent / guardian if you are at home

● Students should never share personal information about themselves or others, including phone numbers, addresses, PPS numbers and birth-dates over the Internet without adult permission

● Students should never agree to meet in real life someone whom they meet online, without parental permission.

Cyber-bullying (See Anti Bullying Policy)

Harassing, flaming, denigrating, trolling, impersonating, outing, tricking, excluding, cyber-stalking and creating memes are all examples of cyber-bullying.

● Such bullying will not be tolerated in St Joseph's College.

● Students must not send emails or post comments or photos with the intent of scaring, embarrassing, hurting, or intimidating someone else

● Engaging in any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges

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, they should contact the ICT Coordinator for clarification.

Violations of this Responsible Use Policy

Violations of this policy in St Joseph's College may have disciplinary repercussions, including:

● Suspension of network and computer privileges
● Notification to parents in most cases
● Detention or additional duties
● Suspension from school and/or school-related activities

- Expulsion
- Reporting of behaviour to the Gardaí
- Legal action and/or prosecution in the event of any disciplinary action, the completion of all class work remains the responsibility of the student.

Email

- Students will use approved class email accounts under supervision by or permission from a teacher.
- Students will not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person.
- Students will not reveal their own or other people's personal details; such as addresses or telephone numbers or pictures.
- Students will never arrange a face-to-face meeting with someone they only know through emails or the internet.
- 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, messaging or other electronic communication fora that have been approved by the school.
- Chat rooms, discussion forums and other electronic communication 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/Social Media

- The school will endeavour to use digital photographs, audio or video clips of focusing on group activities. Photographs, audio and video clips will focus on group activities. Video clips may be password protected.
- Personal student information including home address and contact details will be omitted from school web pages.
- The school website will avoid publishing the first name and last name of individuals in a photograph.
- The school will ensure that the image files are appropriately named – will not use students' names in image file names or ALT tags if published on the web.
- Students will continue to own the copyright on any work published.

Personal Devices

Students using their own technology in school, such as leaving a mobile phone turned on or using it in class, sending nuisance text messages, or the unauthorized taking of images with a mobile phone camera, still or moving is in direct breach of the school's acceptable use policy.

Legislation

The school will provide information on the following legislation relating to use of the Internet which teachers, students and parents should familiarise themselves with:

- Child Protection Procedures for Primary and Post-Primary School 2017
- Children First 2015
- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1998
- Interception Act 1993

- Video Recordings Act 1989
- The Data Protection Act 1988

Support Structures
The school will inform students and parents of key support structures and organisations that deal with illegal material or harmful use of the Internet.

Sanction
An Acceptable Use IT agreement form is in every student's diary and must be signed by both student and parent/guardian. Failure to do so may result in suspension of IT use until agreement with AUP. (See Appendix 1)
Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities.

A review of this policy will take place regularly with the aid of checklist (See Appendix 2)

This Policy was reviewed and ratified on ________________.

Signed: ________________ Date: _____________
Principal

Signed: ________________ Date: _____________
Chairperson BOM

Appendix 1

ACCEPTABLE USE I.T.

St. Joseph's College, Borrisoleigh

Name of Student: ______________________

Class/Year: ______________________

Student

I will use the Internet in a responsible way and obey all the rules explained to me by the school.

Student's Signature: __________________________ Date:

Parent/Guardian

As the parent or legal guardian of the above student,. I understand that Internet access is intended for educational purposes. I also understand 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.

I accept the above paragraph □I do not accept the above paragraph □

(Please tick as appropriate)

In relation to the school website, I accept that, if the school considers it appropriate, my child's schoolwork may be chosen for inclusion on the website. I understand and accept the terms of the Acceptable Use Policy relating to publishing students' work on the school website.

(Please tick as appropriate)

I accept the above paragraph □I do not accept the above paragraph □

Signature: ______________________________ Date: _______________

Address: ______________________________

____

____

Appendix 2

AUP checklist

For an AUP to be robust it needs to be reviewed and updated regularly, taking into consideration implementation issues that may arise. The following is a checklist that may be used when developing or revising an AUP.

1. Have AUP implementation issues arisen since the AUP was designed/revised?

2. Have these issues been discussed with parents, students and teachers and incorporated into an updated AUP?

3. Given that an AUP is in place, can the school confidently address the following scenarios?
   - A student is found using a chat room to arrange a face-to-face meeting with a friend.
   - The school uses filtering software but a student accidentally accesses a pornographic website while in your care.
   - A student publishes defamatory information on a personal website about a peer.

4. Has the AUP had a positive impact on curriculum delivery?

5. Has internal or external expertise assisted the formulation or reformulation of the AUP?

6. Has the school discussed the use of the Internet with parents and guardians?

7. Has the AUP as a code of Internet use transferred to home use?

8. Does an open dialogue exist between students and teachers relating to Internet misuse and safety issues?

9. Are teachers' and students' Internet safety training needs being met?