Acceptable Usage Policy

Coláiste Iósaef

Acceptable Use Policy (AUP) for Computer and Internet Usage in Coláiste Iósaef

An Acceptable Usage Policy (AUP) is a document that addresses all rights, privileges, responsibilities and sanctions associated with the Internet, computer and personal device use. The school aims to maximise learning opportunities while reducing associated risks and will endeavour to advise students on good practice and safe use of the Internet.

The policy should be read in conjunction with the school's Code of Behaviour and Anti-Bullying Policy.

Computing Facilities/Internet Access via Mobile Devices

Students are encouraged to make use of the school's computing facilities for educational purposes and are expected to act responsibly and to show consideration for others.

Use of Technology

Any technology that can be used to store, transmit or manipulate data, such as SMART devices e.g. phones, watches, Tablets (Android, iOS, Windows & mobile devices), Personal Digital Assistants (PDAs), and USB media, should be used responsibly and in accordance with the Acceptable Use Policy (AUP), even when not used with school equipment or network. These devices are not allowed to be used during class, house exams or State Examinations unless under the strict instruction of the teacher and for the specific purpose only.

Conventional norms of behaviour apply to computer-based information technology just as they would apply to more traditional media.

Rationale

The school supports and respects each family's right to decide whether or not to allow access to the Internet through the school network.

School computers and Internet connection should be used to enhance learning. Internet use and access is considered a school resource and privilege. If the school's AUP is not adhered to, this privilege will be withdrawn and appropriate sanctions may be imposed. The AUP agreement (appendix 1) must be signed by students and their parents or guardians and returned to the school before access is granted.

Usage of the Internet therefore requires responsibility on the part of the user and the school's staff. These responsibilities are outlined in the school's AUP.

As part of the school's educational programme students may also be offered WiFi access to the Internet which is monitored via the Oide and LCETB (Formula Networks) Content Filtering Service.

The Internet is a global computer network which is not controlled by any organisation. This means that information may change, disappear, and be controversial or potentially harmful. Although the school actively

seeks to promote safe use of the Internet, it recognises the possibility that students may accidentally or deliberately access objectionable material.

Students and their parents/guardians are advised that activity on the Internet is monitored and that these records may be used in investigations, court proceedings or for other legal reasons.

User Responsibilities

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

1. Students will be made aware of issues relating to Internet safety and the fact that the school will regularly monitor students' Internet usage.
2. Internet sessions will always be filtered through the Oide and LCETB Content Filtering Service. In class situations the member of staff supervising Internet sessions will endeavour to ensure compliance with this policy.
3. Students will be informed about what is acceptable and what is not acceptable in order to minimise the risk of exposure to inappropriate material.
4. Uploading and downloading of non-approved software will not be permitted on devices.
5. CD ROMs, DVDs and USB drives or any other devices cannot be used without permission on school devices/hardware.
6. No electronic storage media or device may be connected to the school network without permission from the ICT Department and/or school management.
7. Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.
8. Students should not visit Internet sites that contain inappropriate materials (e.g. obscene, illegal, hateful or otherwise objectionable materials).
9. Students must report to a teacher any material of the above nature that they encounter whether deliberately or accidentally.
10. The school will keep a record of all students who are granted Internet access.
11. Students must not disclose or publicise personal information about themselves or others.
12. Students will be aware that any usage, including distribution or receiving of information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.
13. Students will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).
14. When using the Internet, all users must comply with all copyright, libel, fraud, discrimination and obscenity laws, and all network users are expected to communicate in a professional manner consistent with the rules of behaviour governing employees in the education sector.
15. Mobile phone, voice and text, SMS messaging or any device that uses instant messaging use by students is not permitted.

16. The use of the microphone or recording function on any device is strictly prohibited except under the direction and permission of the teacher.

Reasonable Use

Our school utilises Google Meet and Zoom(staff & BOM only) for teleconferencing during periods of school closure. Distance learning is a way of learning remotely without being in regular face-to-face contact with a teacher in the classroom. There are many benefits to teaching and learning in this way, and students and teachers have the tools and expertise to use teleconferencing to sustain learning.

Our school provides a Google Meet video conferencing option for our students and staff in learning and teaching (GSuite Education). It is expected that students and staff will use the platforms in a professional and ethical manner for the purpose of teaching, learning and assessment.

The use of teleconferencing requires students and teachers to observe the following rules in order to ensure that both staff and students benefit from this way of teaching and learning. Students and Staff should never;

1. Post, stream or transmit any content, including live video, that violates this Policy in such a way that is offensive to students / staff.
2. Do anything illegal, facilitate any illegal activity, or promote violence.
3. Do anything that threatens, exploits or otherwise harms children or fellow students.
4. Engage in any activity that is harmful, obscene, or indecent. This includes offensive gestures, displays of nudity, violence, pornography, sexually explicit material, or criminal activity.
5. Engage in any activity that is fraudulent, false, or misleading.
6. Engage in any activity that is defamatory, harassing, threatening or abusive.
7. Store or transmit any data or material that is fraudulent, unlawful, harassing, libelous, threatening, obscene, indecent or otherwise inappropriate.
8. Send unauthorized messages or irrelevant material.
9. Misrepresent a user's identity or affiliation with any entity or organization, or impersonate any other person.
10. Harvest, collect, or gather user data without consent.
11. Violate or infringe any intellectual property or proprietary rights of others, including copyrights.
12. Violate the privacy of others or distribute confidential or personal information of others.
13. Engage in any activity that is harmful or disruptive to the operation of on-line classes. This includes transmitting viruses, malware or other malicious or destructive code or using tools that mask IP address location or to otherwise circumventing restrictions on use due to regulations or account closures.

If school authorities are made aware of any abuse or infringement on these rules, the school will investigate the issue and take immediate, appropriate action where warranted in line with the school's Code of Behaviour.

Intellectual Property Rights

Subject specific educational resources designed by staff remain the property of the school teaching staff who authored them. Students will be allocated a license to use them for as long as they are taking that subject or up to Leaving Certificate level. It is strictly forbidden to share school developed educational resources with another person not associated with the school or download them for any other use.

Email Usage

1. Use of email may be subject to monitoring for security and/or network management reasons.
2. Students will receive an @cik.ie school email address (e.g johnsmith23.student@cik.ie). This is the only email a student is permitted to use for school purposes, sending work to a teacher, etc. Personal email addresses should not be used.
3. Students may not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate any other person/s.
4. Students must immediately tell a teacher if they receive an offensive email.
5. The forwarding of chain letters/emails is forbidden.
6. Students should note that sending and receiving email during class time is subject to permission from their teacher.
7. If representing the school, any email to an external party should be written carefully and authorised by a member of staff before sending.
8. Students must not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.
9. Students must never arrange a face-to-face meeting with someone they only know through emails or the Internet.
10. Student email accounts will be deleted once a student has left the school. This is will be done in a period after 3 months of the student leaving the school.

Chromebooks and PC's

At Coláiste Iósaef, we believe in providing access to education technology, tools and resources. Essential to this effort is our commitment to rethink teaching and learning. We have made a huge investment in infrastructure (WiFi, Chromebooks, etc.) and services to ensure the best education possible for our students. We are expanding educational opportunities for teachers and students that will help ensure equitable access to instructional tools and resources in school and at home.

Students will develop skills through the use of Chromebooks/PC's, a content-focused curriculum and collaborative technology tools. The lessons learned and the insights gained through this, will provide an effective and feasible blueprint for future implementations throughout Ireland.

We acknowledge the support of our parent population, with the Chromebook initiative, and anticipate that this support will continue.

The policies, procedures and information within this document apply to all Chromebooks, PC's and IT equipment used at Coláiste Iósaef including any other device considered by Staff to come under this policy. Teachers may also set additional requirements for use in their own classrooms.

The use of 3G/4G/5G and cellular devices are not permitted.

Chromebooks and PC's will only be used during class time under the supervision of the teacher.

Chromebooks will be distributed during class by the teacher.

Students are allowed the use of these devices exclusively for school based instructional use.

The purpose of the Chromebook facility and ICT usage is to enhance classroom learning.

Expectations

1. Students will practice extreme care when using Chromebooks, PC's and other equipment.
2. Students are only permitted to use Chromebooks/PC's during class time and under the direct supervision of their teacher.
3. Students are expected to uphold all copyright laws, values and protect the privacy of information.
4. Students must not share passwords or account information with anyone else.
5. Students must return Chromebooks after use, to the allocated slot in the correct trolley and plug in to the appropriate power adapter.
6. Students will leave IT rooms the way they found them.
7. Students will inform a member of staff if they find anything out of place.
8. Students will not rearrange any IT connections e.g. Mouse, ethernet cables etc.
9. Students will only enter an IT room when a teacher is present.

In exceptional circumstances the school may agree to loan a student a device for off-site use. In such circumstances the device continues to remain the sole property of the school and must be returned immediately upon request. The student agrees to take all reasonable care of the device when it is in their possession and accepts that this policy continues to apply at all times. Such a device is for the sole use of the student and should not be used by others (for example: family members, friends, fellow students, etc).

Unacceptable Conduct (includes but is not limited by the following)

1. Use of the Chromebook/PC for illegal activities, including copyright or contract violations, downloading inappropriate content including viruses, file sharing software, hacking programs or any other form of inappropriate content.
2. Disabling, bypassing, or attempting to disable or bypass any system monitoring, filtering or security measures.
3. Electronically posting personal information about yourself or others. (i.e. address, phone, photos)
4. Maliciously altering data, the configuration of the Chromebook/PC, the files of another user, accessing restricted network files or any other form of technological vandalism.

5. Engaging in any conduct that is considered illegal under Irish, county, local or any other Government law.
6. Wasting or abusing resources through excessive use of bandwidth or unauthorized system use (e.g. Internet radio, online gaming, downloading media files)
7. Students are responsible for any Chromebook/PCs that they use. If a student damages a Chromebook, PC or other IT equipment, the onus to repair the equipment or device will fall on the student and parent/guardian. These repairs must be carried out by a recommended authorised supplier as agreed by the school.

Managing your files and saving your work

Students should save their work on their 'CIKdrive' Google Drive account, school server or other cloud based computing service.

Students must not avail of storage space on any Chromebook or school PC/device – any work saved in this way will be deleted on signing out of the device or when reimaging.

It is the students' responsibility to ensure that their work is not lost due to mechanical failure or accidental deletion.

School responsibilities

Provide Internet access at school

Provide an academic Gsuite and email account (e.g. username@cik.ie) to its students.

Provide Internet blocking of inappropriate materials while using the school network.

Provide staff guidance to aid students in doing research, academically related activities and how to ensure student compliance with the acceptable usage policy.

Student responsibilities

Read, understand and follow this AUP Policy.

Use all Chromebooks/Computers/Devices in a responsible and ethical manner.

Obey general school rules concerning behaviour and communication that applies to Chromebook/Computer use.

Physical damage to devices should be reported immediately to school staff.

Usernames And Passwords for Students

1. Upon student and parent/guardian signature on the Acceptable Use Policy agreement (appendix 1) students will receive a username and password. This will grant them access to the schools network and their own personal Gsuite (CIKdrive) account.
2. Students must not share their username or password with another person in or outside school.
3. Students will keep their username and password in a secure and private location.

Mobile Phones

Students are not permitted to use mobile phones once the school day begins at 8.50am (first bell).

Students can bring a phone to school but it must be switched off after 8.50am. It may be switched back on at the end of the school day, should a student need to make contact with a parent/guardian, etc.

In some instances, a mobile phone may be used under the direct instruction and supervision of a teacher, these may include taking a picture of a project for the brief write, etc.

If it is necessary to contact a parent, this must be done through the school office with permission from a students Year Head, Deputy Principal or Principal.

The school has a policy of 'not seen, not heard, not taken'.

Any student who is in breach of this rule will have their mobile phone confiscated.

Mobile phones will only be returned at the end of the school day by the Deputy Principal. Repeated infringements of this will incur further sanctions (including but not limited to banning the student from bringing a mobile phone to school).

Mobile Chromebooks and Devices

Only approved school devices will be able to access the secure school wireless network through their normal school login and password, after accepting this AUP.

Please note that privately owned devices (Tablets, Laptops, etc.), should only be used with the wireless network (with permission from the Principal, IT department, year head and teacher) and under no circumstances should these devices be physically plugged into the school network connection points.

Class Based Use of Approved Personal Devices (BYOD):

Student Responsibilities

. The following applies to these devices:

1. The usage of any personal mobile device must be pre approved by the Principal, ICT department, Year head and class teacher.
2. Any personal mobile device is granted only in specific circumstances and is subject to inspection by administration and teaching staff at any time without notice.
3. Students approved devices used in a classroom context must arrive at school each day fully charged. The school is under no obligation to supply a charging facility. Students must take their device home each day and it must not be left on campus.
4. Where a device is a replacement for paper textbooks, students should note that writing materials are still a requirement. Students must have the necessary writing materials (pen / paper).
5. Devices are to be kept within a suitable protective case and are securely stored away when not in use, for example at break, lunchtime or school related activities.
6. Students must not allow anyone to use the mobile device other than their parents, teacher or other school- appointed person.
7. Games, entertainment or social media may not be used during class time or at any other time within the school except under the direction of a teacher.
8. Report any problems, damage or theft immediately to your teacher, Year Head or IT coordinator. Devices that are stolen must be reported immediately to the school administration.
9. Students must not go home from school without reporting any damage or interference that may have occurred during the school day. If you do so, school management will presume that the damage and/or interference took place outside of school time.
10. The use of 3G/4G/5G mobile WiFi on a device is not allowed. Only the school network is to be used by students while at school. Access to the school network must only be with the students own login and username details.
11. All work must be backed up and secured.
12. Mobile devices are to be left at home or in a secure place when students are on tours, trips and activities.
13. Students must ensure that mobile devices are not connected to any school-owned equipment without the permission of the school Principal, Deputy Principal or an appropriate ICT staff member.
14. Students must not create, transmit, re-transmit or participate in the circulation of content on their devices that attempts to undermine, hack or bypass any hardware and software security mechanisms that have been implemented by the ICT department, or the school. The school's internet or email accounts must not be used for financial or commercial gain.
15. Students must not take photos or make video or audio recordings of any individual or group without the express permission of each individual (including parent/guardian consent for minors) being recorded and the permission of an appropriate staff member.

16. Students and their parents/guardians are solely responsible for the care, maintenance and security of their devices.
17. Students must have a supported operating system and current antivirus software, if applicable, installed on their device and must continue to maintain the latest service packs, updates and antivirus definitions. Do not jailbreak the device i.e. modify (a smartphone or other electronic device) to remove restrictions imposed by the manufacturer or operator, e.g. to allow the installation of unauthorised software.
18. Students are responsible for ensuring that the operating system and all software on their device are legally and appropriately licensed.

Lost, Damaged or Stolen Device

If you lose or damage your device you must inform the ICT Co-ordinator /Year Head / Deputy Principal / Principal immediately so that your device may be tracked, where possible.

The school is not responsible for loss, the financial loss, damage or otherwise to your device or loss of data / content.

Technical Support

The school is under no obligation to provide technical support for hardware or software. The school may choose to provide this service to students if there are sufficient resources available in the school.

Insurance

The school cannot take any responsibility for the safe working, repair or security of personal devices whilst on, or in transit to and from the school campus.

It is each student's responsibility to ensure that any electronic devices brought onto the school campus are suitably insured. The School's insurance DOES NOT cover these items. Insurance is the responsibility of parents/guardians and students.

It is strongly recommended that insurance cover is acquired for any devices used on the school campus.

Parental Responsibilities

- Parents are requested to inspect their device each evening to ensure that it is in good working order.
- Parents should report, immediately, any damage, interference or issues relating to ownership, possession or use of the device to school management via the school office.

- Parents should inspect the device, any installed apps or programs on a regular basis to ensure that there is no inappropriate material.
- Parents are responsible for providing device insurance on an annual basis and MUST return any school issued device and accessories in the same condition as received.

Sanctions for Breach of Acceptable Use Policy (AUP)

1. Misuse of the computer privileges may result in disciplinary action, including written warning, withdrawal of access privileges and, in extreme cases, suspension or expulsion if warranted under the school's Code of Behaviour. It is school policy to report any illegal activities to the appropriate authorities.
2. This Acceptable Use Policy (AUP) governs the use of the school's computer facilities and wireless network by students. Parents/Guardians who object to all or part of this AUP should inform the Principal in writing and by returning the agreement page unsigned. Once signed, parents are deemed to have accepted the contents of the AUP as a condition of the use of the computer facilities by their child.
3. Where the school has reasonable grounds to suspect that a device contains data which breaches the AUP, the school may confiscate the device for the purpose of confirming the existence of the material.
4. Access to the school Wi-Fi network will be withdrawn with immediate effect for failure to adhere to this AUP, or any other applicable school policy or guideline.
5. Access to the school network may be restricted or withdrawn at any time, without notice, to ensure that the integrity and security of the network and/or other users is not compromised.
6. All material on devices must adhere to the schools AUP. The access, sending, uploading, downloading or distribution of offensive, threatening, pornographic, obscene, or sexually explicit materials is strictly prohibited and will result in disciplinary action.
7. The school reserves the right to refer to external agencies in the event of illegal activity.

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.

- Have AUP implementation issues arisen since the AUP was designed/revised?
- Have these issues been discussed with parents, students and teachers and incorporated into an updated AUP?

Given that an AUP is in place, can the school confidently address the following scenarios?

i. A student is found using a chat room to arrange a face-to-face meeting with a friend.

ii. The school uses filtering software but a student accidentally accesses a pornographic website while in your care.

iii. A student publishes defamatory information on a personal website about a peer.

- Has the AUP had a positive impact on curriculum delivery?
- Has internal or external expertise assisted the formulation or reformulation of the AUP?
- Has the AUP as a code of Internet use transferred to home use?
- Does an open dialogue exist between students and teachers relating to Internet misuse and safety issues?
- Are teachers' and students' Internet safety training needs being met with regards to the policy and what it represents.

Review Process

The policy will be reviewed in line with Coláiste Iósaef procedures regarding policy reviews and updates.

Signed: _____ Signed: _____

(Chairperson of Board of Management) (Principal)

Date: _____ Date: _____

Date of Policy Review: _____

EXAMPLES OF POSSIBLE ACTIVITY / SANCTIONS (this list is not exhaustive)

Activity	***Sanction***
Possessing, viewing and / or distributing unacceptable material i.e. images, sound or video clips via email, USB, shared resources or other means e.g. YouTube / Vimeo /Social Media sites or Apps e.g. Snapchat, Instagram.	• Note on VSWare for inappropriate conduct. • After school detention, suspension or other sanction up to and including expulsion. • Gardai informed where appropriate.
Installation or distribution of viruses / malware etc.	• WiFi privilege removed indefinitely and Gardai informed. • After school detention, suspension or other sanction up to and including expulsion.
Connecting to the schools network by bypassing filtering / security measures (using software, proxy server websites etc.).	• The automatic removal of WiFi privileges. • Access to the school network will be removed indefinitely • After school detention, suspension or other sanction up to and including expulsion.
Taking of photos on personal ICT devices without expressed permission.	• After school detention, suspension or other sanction up to and including expulsion.
Charging devices without permission.	• Initial warning and note sent home. • Repeated offence - loss of IT privileges.
Accessing the Internet in class without teacher permission.	• Note on VSware for breach of ICT AUP. • After school detention/phone call home • Repeated offence - loss of IT privileges.

The following websites offer support and advice in the area of Internet Safety:

Make IT Secure - http://makeitsecure.org	NCTE - http://www.ncte.ie/InternetSafety
Safe Internet - http://www.saferinternet.org	Webwise - http://www.webwise.ie/