Student Acceptable Use, IT & Mobile Device Policy

The following Acceptable Use Policy has been developed to reflect the school's commitment to the correct and proper use of its ICT resources.

021 496 2025

St. Patrick's Road,
Ballyphehane, Cork, T12
XT96.

info@cercork.ie

DP/09/2023

APPROVED BY
Board of Management

REVISION DATE
20 October 2023

Student Acceptable Use, IT & Mobile Device Policy

Document Title

Student Acceptable Use, IT & Mobile Device Policy

Revisions

No.	Status	Author(s)	Approved By	Office	Issue Date
Rev 01	Release	Ark www.arkservices.ie	Ark	Cork	October 2023

Circulation

Position	Office	Issue Date	Method
Senior Management	Coláiste Éamann Rís	October 2023	Email
Board of Management	Coláiste Éamann Rís	October 2023	Email
Students	Coláiste Éamann Rís	October 2023	Email

Table of Contents

Student Acceptable Use, IT & Mobile Devices Policy

Coláiste Éamann Rís has invested significantly in the provision of technologies to aid teaching and learning as well as facilitate remote teaching and learning (where needed) in the school. Coláiste Éamann Rís (School) is committed to the correct and proper use of its ICT resources in support of its teaching & administrative functions.

The inappropriate use of information and communication technology (ICT) resources could expose the school to risks including virus and malicious software attacks, theft and unauthorized disclosure of information, disruption of network systems and / or litigation.

The purpose of this policy is to provide students as users of its ICT resources with clear guidance on the appropriate, safe and legal way in which they can make use of the school's ICT resources.

Scope
This policy represents the school's position and takes precedence over all other relevant policies. The policy applies to:

- All ICT resources provided by the school.
- All students as users of the school's ICT resources.
- All use (both personal & school related) of the school's ICT resources.
- All connections to (locally or remotely) the school network Domains (LAN/WAN/Wi-Fi).
- All connections made to external networks through the school network.

General Principles
The acceptable use of the school's ICT resources is based on the following principles:

- All ICT resources and any information stored on them remain the property of the school.
- Students must ensure that they use ICT resources at all times in a manner which is lawful, ethical and efficient.
- Students must respect the ICT devices and equipment provided for their use and take all reasonable steps to prevent damage, loss or misplacement.
- Students must respect the rights and property of others, including privacy, confidentiality and intellectual property.
- Students must respect the integrity and security of the school's ICT resources.

Breaches of this policy may be treated as a matter for discipline. Depending on the seriousness of the breach this will be dealt with by the Principal in accordance with the School's Code of Behaviour. For breaches which do not warrant such action, those involved will be advised of the issue and given a reasonable opportunity to put it right.

Signed: _____
Chairperson Board of Management

Signed: _____
Principal

Date: _____

Date: _____

2. Objectives

- Protect and maintain the integrity of the facilities and make communications reliable.
- Support teaching and learning.
- Implement best practice in the appropriate use of ICT Resources.
- Ensure that users engage only in the appropriate uses of ICT Resources to meet the needs of staff and students.

3. Responsibilities – Board of Management

Our entire school community have a role in implementing the Acceptable Use Policy.

- The Board of Management will approve the policy and ensure its development and evaluation.
- As new technologies are developed that may prove valuable to our teaching and learning goals, to evaluate and provide access to them if necessary.
- To consider reports from the Principal and the ICT Department on the implementation of the policy.
- Maintain an approved list of technologies.

4. Responsibilities – Senior Management

Our entire school community have a role in implementing the Acceptable Use Policy.

- Senior Management will be responsible for the dissemination of the policy including where relevant the application of sanctions.
- To oversee implementation of the policy.
- To establish structures and procedures for the implementation of the Acceptable Use Policy.
- To provide parents with the school's Acceptable Use Policy. To notify all parties when the policy has been updated.
- To ensure that users understand that failure to adhere to this Acceptable Use Policy will result in the loss of privilege and/or disciplinary action.
- To monitor the implementation of the policy.

5. Responsibilities – ICT Department

Our entire school community have a role in implementing the Acceptable Use Policy.

- The ICT Department will be responsible for the technical implementation of the policy.
- To provide input on the implementation of the policy.
- To establish structures and procedures for the implementation of the Acceptable Use Policy.
- To make the necessary technical arrangements in order to demonstrate the AUP in practice.
- Where the AUP has been breached, report the breach to the Principal.
- To monitor the implementation of the policy.

6. Responsibilities – Teaching Staff

Our entire school community have a role in implementing the Acceptable Use Policy.

- To instruct students in the appropriate use of computer and internet resources.
- To monitor the use of ICT resources.
- To record any violations of the Acceptable Use Policy and inform the Principal.
- To impose appropriate sanctions for violations of the Acceptable Use Policy.
- To report incidents of online bullying and be mindful of the obligations under Child Protection Guidelines.

7. Responsibilities – Students

Our entire school community have a role in implementing the Acceptable Use Policy.

- To agree to exhibit responsible behaviour in the use of all ICT resources.
- Take personal responsibility for not accessing inappropriate material on the internet.
- To accept that Coláiste Éamann Rís is not responsible for materials, or information of any kind, found or acquired on the network.
- To accept that violation of this Acceptable Use Policy may result in access privileges being revoked and that appropriate school discipline and/or legal action may be taken at the discretion of Coláiste Éamann Rís.

8. Responsibilities – Parents / Guardians

Our entire school community have a role in implementing the Acceptable Use Policy.

- To become familiar with the school's Acceptable Use Policy and to discuss it with their child.
- To accept responsibility for supervision, if and when a student's use of email and the internet is not in a school setting. Parents are obliged to support the school's Acceptable Use Policy.

9. Routine Monitoring

The school reserves the right to routinely monitor, log, audit and record any and all use of its ICT resources for the purposes including:

- Helping to trace and resolve technical faults.
- Protecting and maintaining network and system security.
- Maintaining system performance and availability.
- Ensure the privacy and integrity of information stored on the network.
- Investigating actual and suspected security incidents.
- Preventing, detecting and minimising inappropriate use.
- Protecting the rights and property of the school, its staff, students and wider school community.
- Ensuring compliance with other school policies, current legislation and applicable regulations.

Whilst the school does not routinely monitor an individual's use of its ICT resources it reserves the right to do so when a breach of its policies or illegal activity is suspected. The monitoring may include, but will not be limited to individual login sessions, details of information management systems and records accessed, contents of hard disks, internet sites visited, time spent on the internet, and the content of electronic communications.

Coláiste Éamann Rís will at all times seek to act in a fair manner and respect the individual user's right for the privacy of their personal information under the Data Protection Act 2018.

Information collected through monitoring will not be used for purposes other than those for which the monitoring was introduced, unless it is clearly in the users interest to do so or it reveals activity that the school could not be reasonably expected to ignore, for example a user found to be viewing, downloading or forwarding pornography must be reported to Gardai.

Individual monitoring reports will only be accessible to the appropriate authorised personnel and will be deleted when they are no longer required.

10. User Accounts & Passwords

Where appropriate, individual students will be granted access to the school's ICT resources.

- Each authorised user will be assigned an individual user access account name and password set which they can use to access a particular ICT resource.
- Each user is responsible for all activities performed on any ICT device, management information system or software application while logged in under their own individual access account and password.
- Students must ensure all passwords assigned to them are kept secure.
- Students should not use the same password for their personal accounts i.e. social media as their school supplied accounts.
- Passwords must contain a minimum of 8-12 characters including a combination of letters (both upper & lower case), numbers (0-9) and at least one special character (for example: ", £, $, %, ^, &, *, @, #, ?, !, €).
- Students who suspect their password is known by others must change their password immediately.

11. ICT Devices & Equipment

All ICT devices and equipment are purchased through the agreed channels.

- All ICT devices and equipment provided to students remain the property of the school.
- Students must not remove or borrow school ICT devices or equipment without the authorisation of the ICT Department.
- Students must not alter the hardware or software configuration of any school ICT device or equipment without the prior authorisation of the ICT Department.
- Students must take due care when using school ICT devices and equipment and take reasonable steps to ensure that no damage is caused to the ICT device or equipment.
- Student must report all damaged, lost or stolen school ICT devices and equipment to their Class Teacher.
- ICT Equipment must be returned by students before they leave the school. In addition, the school will then disable access to school software applications within 1 month.
- The school reserves the right to remove any ICT devices and equipment from the network at any time, for reasons including but not limited to (1) noncompliance with school policies, (2) the ICT device or equipment does not meet approved specification and standard, or (3) the ICT device or equipment is deemed to be interfering with the operation of the network.

12. Mobile Computer Devices & Smart Devices

- Students must take all reasonable steps to ensure that no damage is caused to the device and the device is protected against loss or theft.
- School devices will be password protected in accordance with the user accounts and password policy.
- Passwords used to access school laptops, mobile computer devices and smart devices must not be written down on the device or stored with or near the device.
- All school supplied devices will be set up with a password / pin code / swipe gesture to gain access.

13. Access to School Network

Access to school network domains and network resources is controlled and managed by the ICT Department.

- Access rights and privileges to the school network domains and network resources will be allocated based on the specific requirement of each student through the ICT Department.
- Access to school network domains will be controlled by the use of individual user accounts.
- Students must not:
  - Disconnect any school ICT devices, equipment or removable storage devices to or from a school network domain without the prior authorisation of the ICT Department.
  - Connect any school ICT devices and equipment, laptop or smart device to an external network without the prior authorisation of the ICT Department.
  - Connect any ICT devices and equipment, laptop, smart device, mobile phone device or removable storage device which is their personal property and is not owned or leased by the school to a school network domain without the prior authorisation of the ICT Department.

14. Information Storage

- Students are not permitted to store non-school personal information (i.e. information which is of a personal nature and belongs to the student and not the school) on their school ICT Resource / Device.
- Photographic, video and audio recordings which are taken as part of school business must be transferred from the recording device (i.e. digital camera, video camera, mobile phone, tape recorder etc) onto a school network server or cloud as soon as is reasonably practicable.
- When the transfer is complete the photographic, video or audio recording on the recording device should be deleted.

15. Students Use of Technology - General

- Internet sessions will be supervised by a teacher, where possible.
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material.
- The school can monitor students' Internet usage.
- The use of non-approved software will not be permitted.
- Virus protection software will be used and updated on a regular basis.
- The use of digital storage media (e.g. Cloud storage, memory sticks/cards, personal USBs, CDROMs etc.) in school requires a teacher's permission.
- Students will always treat others with respect and will not undertake any actions that may bring the school into disrepute.
- Students are forbidden from opening apps in class or going online, unless instructed to do so, and only for the purposes instructed by a teacher.
- Students will not use school supplied ICT resources except for approved personal reasons.
- School email accounts should not be used to sign up to other non-educational apps or websites.

16. Use of Email

- Students will use their school email account for educational use, and will not use their personal email accounts to communicate with teachers.
- Students will use school supplied school email accounts for communications with teachers (using the teacher's school email account).
- 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, telephone/mobile phone numbers or pictures.
- School email accounts for student leavers will be de-activated 12 months after leaving school. Leavers must remove all third-party accounts associated with their email account.
- School accounts should not be used for registering third party sites without teacher approval i.e. CAO.

17. Internet Use

- Internet access is provided by PDST NCTE (School-Filtered Broadband) for teaching and learning.
- Another Broadband line is also available for non-teaching and learning activities.
- Appropriate school Wi-Fi is available to all students and staff. The Wi-Fi is password protected for security reasons and to help ensure child and data safety.
- No other networks/personal data (3G, 4G, Personal Hotspots etc.) may be used by students during class time, and all Internet sessions as part of any school activity, unless under the direct instruction / supervision of a teacher.
- Students will not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise explicit or objectionable materials.
- Students will report accidental accessing of inappropriate materials in accordance with school procedures.
- Students will use the Internet for educational purposes only during class time, and all Internet sessions as part of any school activity.
- Students will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures. Students should retain their usernames and password securely.
- Students will never arrange a face-to-face meeting with someone they only know through emails or other online communication without the permission of their teacher.
- Students will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement). Students will be required to exercise care and attention in citing sources, references, photos/images and to acknowledge copyright if some material is used in their work. When downloading material from the Internet, students will take reasonable care to ensure that the material is from safe sources, copyright-free (where possible) and referenced appropriately.
- Students will never disclose or publicise personal information in relation to themselves or others.
- Downloading of materials or images by students, which is not relevant to their studies, is in direct breach of this Acceptable Use Policy.
- Students should note that any usage, including distributing or receiving information, school related or personal, may be monitored for unusual activity, security and/or network management reasons.
- School Devices will be available to students. At all times, students must use their school login details and their own storage area on the school supplied cloud.
- It is strictly forbidden for students to delete the work or files of other students from folders on the school network.
- It is strictly forbidden for any student to attempt any act of hacking or other form of sabotage that could compromise the security of the school's network and digital data. Any such action will result in a serious sanction being imposed, including the option to suspend or expel the student involved.
- Students must log out of their own accounts at the end of each Internet session. Students are not permitted to access the school accounts of other students. In the event where a student accesses a school device and finds another student has not logged out, the student accessing the device must log the other student out before proceeding to use the device. The student should also inform the relevant teacher.

18. Protocol for Remote Learning & Live Classes

Should the school need to revert to a remote teaching / learning approach in light of Covid-19.

- Each teacher and student will be assigned an individual account, username and password which they can use to access a particular ICT resource.
- Only the individual to whom the account was assigned is permitted to use such account i.e. Each school account is for the sole use of the teacher / student only.
- The school will only correspond with the account holder, and should there be a breach of this policy, the school will suspend the account indefinitely.
- Only teachers are permitted to record live classes.
- Students are expected to conduct themselves with respect for both the teacher and their classmates.

When broadcasting classes live, staff should be conscious of the two options available to you:

- Option 1: Choose a window to share that specific program and its content, (preferable option as it restricts the viewers visibility to one dedicated program).
- Option 2: Select Desktop to share everything on your screen (which can lead to inadvertent sharing of information).

Take care to not display any personal data i.e. close down other applications, email or documents which contain personal data prior to showing your screen / recording classes.

19. Cyber Bullying

- Cyber-bullying is defined as using social network sites, internet, email, etc to demean, humiliate, exclude, or otherwise undervalue another person through direct or indirect methods.
- Any incident involving a student, current or recent past, as perpetrator or victim, is of concern, but especially when both perpetrator and victim are students, current or recent past. Equally, social comment about a member of staff which falls under the categories listed above will not be tolerated.
- Cyber-bullying in any form is a very serious issue and will not be tolerated. Any student who experiences cyber-bullying must report it to the school. Any report of cyber-bullying will be taken seriously by the school and appropriate investigative procedures followed, in keeping with the school's Anti-Bullying Policy. Sanctions will be applied, and guidance/counselling offered to students involved in cyber-bullying, in the interest of their well-being.
- Coláiste Éamann Rís draws a distinction between incidents which originate from within the school environs and those which occur outside. While the same standards apply at all times and in all places, it needs to be recognised that the school cannot be held responsible for students' actions when not on the premises.
- Coláiste Éamann Rís takes seriously the responsibility of regularly informing students about online citizenship and best practice in the area of internet usage. Our school values parents' support in reinforcing best practice in this area.

20. Use of Social Media

- The purpose of having school social media accounts include:
  - Communication with the whole school community, especially parents / guardians, regarding specific school information, events & activities.
  - Encourage parent / guardian involvement.
  - Communication with new or prospective parents / guardians.
  - Communication and engagement with the wider community regarding the positive advertisement and marketing of our school.
  - Communication and engagement with other schools and accounts with similar educational interests.
  - Monitor and regulate the school's online presence.
- Only official school social media accounts, or social media as instructed by a teacher, may be accessed by students during class time, and all Internet sessions as part of any school activity.
- Students' personal social media accounts may not be accessed during class time, and all Internet sessions as part of any school activity or using the log-in details ascribed by the school.
- Users should not post anything on school social media channels that could be deemed as offensive – inappropriate or harmful comments/content will be removed immediately.
- Students will not attempt at any time to connect with any member of staff on that staff member's own personal social media account(s).
- Students should not ask to become "friends" with or "follow" staff as failure to respond may cause offence.

School Website / Social Media Accounts

- Students' work will appear in an educational context on Web pages with a copyright notice prohibiting the copying of such work without express written permission.
- Personal student information, including home address and contact details, will be omitted from school web pages.

21. Recordings

Recordings

- Only recordings permitted by a teacher in class are allowed.
- Students are forbidden from taking photos, video or sound recordings of anyone in the school (including students, staff, parents and visitors) unless permitted to do so by a teacher, and in accordance with the School's Data Protection Policy and this policy.
- Students must not share such material online without the clear permission of a teacher and only for educational or school promotional purposes.
- Students may be digitally recorded for educational purposes throughout their time in Coláiste Éamann Rís. Such purposes include Classroom-Based Assessments, extra-curricular activities and participation in educational activities.
- Recordings will be stored on school devices (e.g. digital cameras, school smart devices) and reasonable care will be taken to store recordings securely on the device and on the school's network. This includes both subject-related recordings and recordings of extra-curricular activities in which students are engaged.
- Some recordings will be brought to Subject Learning and Review Meetings by teachers in order to discuss and determine appropriate grade descriptors. Where it is necessary to store such recordings, reasonable care will be taken by teachers to ensure the safe-keeping of such recordings on the school server and / or school cloud.
- All recordings will take place in line with the Child Safeguarding Statement and Child Protection Procedures.
- Subject Learning and Review meetings will see recordings deleted soon after.
- Recordings (e.g. photographs, short video clips) may also be taken of school and extra-curricular activities and events- in the interest of creating a pictorial as well as historical record of life at the school, and may be published on our school website, app, on social media or in brochures, yearbooks, newsletters, local and national news media and similar school-related publications used for promotional purposes of the school, e.g. via the school's official social media accounts. Consent is sought from parents regarding this use of photographs / video recordings on an opt in basis.
- Photographs and video recordings (including CCTV recordings) may also be taken of specific school and extra-curricular activities and events such as sports matches and school trips. The school does not seek consent for this purpose, as it considers that it is necessary for the purpose of its legitimate interests to evaluate and/or monitor those activities/events and to ensure the safety, health and wellbeing of all students, staff, visitors and property.

22. Mobile Devices

- The following should be read in conjunction with the Mobile Phone Usage Policy.
- Students may use their personal mobile device once agreed with the Teacher for educational purposes in specific classes using school approved technologies.
- Once such uses are finished, student personal devices must again be returned securely to their locker.
- Students are responsible for their own technology within the school and on all school linked occasions.
- The unauthorized capture of images, video or audio is in direct breach of this policy.
- It should be noted that it is a criminal offence to use a mobile device to menace, harass or offend another person (Section 10 of the Non-fatal Offences Against the Person Act 1997). Therefore, it may be necessary for the school to inform the Gardaí and/or Child Protection/Support Services in certain circumstances.
- Students using a personal mobile device in school without a teacher's explicit permission, sending nuisance text messages, or the unauthorised taking of images with a personal mobile device, still or moving, are in direct breach of this Acceptable Use Policy and the school's Code of Behaviour. Sanctions may be applied in such cases, as per the school's Code of Behaviour. Use of cameras on digital devices is only permitted with a teacher's permission.
- Where a phone is confiscated by a teacher it will be returned to the student as per the Mobile Phone Usage Policy.
- Students will be reminded of responsible device use and sanctions for misuse from time-to-time at Assemblies.
- Irresponsible or unethical use of personal mobile devices or school Internet will be considered a serious infringement of the Code of Behaviour and disciplinary action will be taken where this applies.
- Day students should charge their personal mobile devices at home.
- In case of illness students should contact home via the school Nurse.

23. Examinations

Examinations

- Mobile phones, Smart watches or other Wifi enabled devices are not permitted in an examination centre. Phones and Smart watches should be secured in locker.

24. Unacceptable Use

The following list should not be seen as exhaustive. The school will refer any use of its ICT resources for illegal activities to the Gardai.

- Political activities, such as promoting a political party / movement, or a candidate for political office.
- To knowingly misrepresent the school.
- To store or transfer confidential or restricted information on a USB memory stick.
- To create, view, download, host or transmit material of a pornographic or sexual nature or which may generally be considered offensive or obscene and could cause offence to others on the grounds of race, creed, gender, sexual orientation, disability, age or political beliefs. Material is defined as information (irrespective of format), images, video clips, audio recordings etc.
- To retrieve, create, host or transmit material which is designed to cause annoyance, inconvenience or needless anxiety to others.
- To retrieve, create, host or transmit material which is defamatory.
- Any activity that would infringe intellectual property rights (e.g. unlicenced installation, distribution or copying of copyrighted material).
- For any activity that would compromise the privacy of others.
- For any activity that would intentionally cause disruption to the computer systems, telephone systems or networks belonging to the school or others.
- Any activity that would deliberately cause the corruption or destruction of data belonging to the school or others.
- Any activity that would intentionally compromise the security of the school's ICT resources, including the confidentiality and integrity of information and availability of ICT resources (e.g. by deliberately or carelessly causing computer virus and malicious software infection).
- The installation and use of software or hardware which could be used to probe or hack the school ICT security controls.
- For the installation and use of software or hardware which could be used for the unauthorised monitoring of electronic communications within the school or elsewhere.
- To gain access to information management systems or information belonging to the school or others which you are not authorized to use.
- Creating or transmitting "junk" or "spam" emails. This includes but is not limited to unsolicited commercial emails, jokes, chain-letters or advertisements.
- Any activity that would constitute a criminal offence, give rise to a civil liability or otherwise violate any law.