ACCEPTABLE USE POLICY

Effective Date: 01.08.20

(01) 628 2299

Roselawn, Ballydowd,
Lucan, Co. Dublin.

admin@colaistephadraig.com

APP01/2020

APPROVED BY
Board of Management

DATE ISSUED
9-Jul-20

TABLE OF CONTENTS

Acceptable Use Policy

Coláiste Phádraig has invested significantly in the provision of technologies to aid productivity and facilitate remote working (where needed) in the school.

Purpose
Coláiste Phádraig (School) is committed to the correct and proper use of its IT resources in support of its teaching & administrative functions.

The inappropriate use of information technology (I.T.) 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 school staff and other users of its I.T. resources with clear guidance on the appropriate, safe and legal way in which they can make use of the school's I.T. resources.

This policy is mandatory and by accessing any I.T. resources which are owned or leased by the school, users are agreeing to abide by the terms of this policy.

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

- All IT resources provided by the school;
- All users (including school staff, students, contractors, sub-contractors, agency staff and authorized third party commercial service providers) of the school's I.T resources;
- All use (both personal & school business related) of the school's IT resources;
- All connections to (locally or remotely) the school network Domains (LAN/WAN/WIFI);
- All connections made to external networks through the school network.

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

- All I.T. resources and any information stored on them remain the property of the school.
- Staff must ensure that they use IT resources at all times in a manner which is lawful, ethical and efficient.
- Staff must respect the rights and property of others, including privacy, confidentiality and intellectual property.
- Staff must respect the integrity and security of the school's IT resources.

Breaches of this policy may be treated as a matter for discipline and depending on the seriousness of the breach and will be dealt with by the Principal in accordance with the School's Code of Behaviour (Students) or Disciplinary Procedure (Staff). 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.

Responsibilities

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

Roles & Responsibilities

- The Board of Management will approve the policy and ensure its development and evaluation.
- The Principal and Deputy Principal will be responsible for the dissemination of the policy; the application of sanctions; and together with the Parents' Association schedule workshops and guest speakers on this topic as appropriate.
- The class teachers will outline to the various classes at an age-appropriate level unacceptable uses of Social Media to students.
- Class teachers and parents will advise children on safe internet use.
- Children and parents will be expected to read, understand and sign an Internet Safety Contract.
- Parents are expected to actively engage with their children, and to educate themselves, on Social Media issues
- Strategies to ensure online safety will be taught as part of an SPHE Anti-bullying programme.
- Teachers will report incidents of online bullying and be mindful of the obligations under Child Protection Guidelines.
- The school community will provide support for students who have been victims of online bullying by implementing our *Anti-Bullying Policy*.

The school may provide students with Internet access, desktop computers, digital imaging equipment, laptop or tablet devices, video-conferencing capabilities, virtual learning environments, online collaboration capabilities, online discussion forums, email and more.
As new technologies emerge, Coláiste Phádraig may provide access to them also. This list is not exhaustible.

Routine Monitoring

The school reserves the right to routinely monitor, log and record any and all use of its IT resources for the purpose of:

Routine Monitoring Purpose

- 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.

While the school does not routinely monitor an individual user's use of its IT 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 systems and records accessed, contents of hard disks, internet sites visited, time spent on the internet, telephone usage and the content of electronic communications.

School 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 Acts 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 child pornography must be reported to Gardai.

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

Personal Use

The School's IT resources are to be used primarily for school business. However at the discretion of Principal occasional personal use may be permitted by a user provided it:

Exceptions

1. Is not excessive;
2. Does not take priority over their school work responsibilities;
3. It does not interfere with the performance and work of the user, other staff or the school;
4. Does not incur unwarranted expense or liability for the school;
5. Does not have a negative impact on the school in any way;
6. Does not involve commercial activities, such as running any sort of private business, advertising or performing work for personal gain or profit;
7. Is lawful and complies with this policy and all other relevant school policies.

The school has the final decision on deciding what constitutes excessive personal use. The school does not accept liability for any fraud or theft that results from a user's personal use of the school's IT resources.

Confidentiality & Privacy

The school as a Data Controller is legally required under the Data Protection Act 2018 to ensure the security and confidentiality of all personal data it processes.

Policy

- In the course of work for the school, you may have access to, or hear information concerning the personal affairs of staff, students or parents. Such information irrespective of the format (i.e. paper, electronic or otherwise) is strictly confidential and must always be safeguarded.
- Staff must respect the privacy and confidentiality of information at all times.
- They must not access information or information systems unless they have a valid school related reason to do so or they have been granted permission by the school.
- Staff must not remove any confidential or restricted information (irrespective of format) from the school without the authorisation of the Principal.
- Confidential and restricted information must only be discussed or shared with others on a strict "need to know" basis.
- Confidential and restricted information must only be discussed or shared with other staff or staff of a government funded agency in accordance with the school Data Protection Policy.
- Confidential and restricted information must only be released and disclosed to other governmental agencies and departments in accordance with the relevant legislation (for example, *Freedom of Information Acts 2003 / Data Protection Act 2018 / Education Act etc.*
- Where it is necessary to release or disclose confidential or restricted information to third parties only the minimum amount of information should be released as is absolutely necessary for a given function to be carried out. Appropriate technical & organizational measures should be adopted to ensure that data is kept secure.
- Confidential or restricted information (irrespective of the format) must not be copied, renamed, deleted or modified without the authorisation of the Principal. This includes information on storage devices and information in transit.
- Personal information belonging to school staff or students must not be used for presentations, training or testing purposes unless it has first been anonymised or psuedonymised otherwise the explicit consent of the school and the individual (as a Data Subject) is required.
- Staff must ensure that all software applications or network access provided to them are not accessed (including internet access) by persons who are not school Staff (i.e. friends, family members and others etc).

Please refer to the school's Data Protection Policy which provides clear guidance regarding the expected use of personal data in the school. The policy is available from the Principal.

User Accounts & Passwords

Where appropriate individual users will be granted access to the school's IT resources which are necessary for them to perform a specific role in the school.

Policy

- Each authorised user will be assigned an individual account name and password set which they can use to access a particular IT resource. Only the individual to whom the account was assigned is permitted to use such account.
- Each user is responsible for all activities performed on any I.T. device, information system or software application while logged in under their individual access account and password.
- Staff must ensure all passwords assigned to them are kept secure. Staff must not write down their password(s) on or near their computer device.
- Staff 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: ", £, $, %, ^, &, *, @, #, ?, !, €).
- Passwords or part of a password must not contain:
  - Any word(s) spelled backwards - (for example: drow, yadnom);
  - Any slang words - (for example: dubs, agro, bling);
  - Any word with numbers appended (for example: deer2000, password2012, Paul2468 etc);
  - Any words with simple obfuscation (for example: p@ssw0rd, l33th4x0r, @dm1n100, g0ldf1sh, etc);
  - Any names of fictional characters - (for example: frodo, shrek);
  - Any common keyboard sequences - (for example: qwerty);
  - Any personal information related to a user - (for example: user name, address, date of birth, school personnel number, car registration number, telephone number);
  - A sequence of consecutive numbers or letters (for example: 12345678, abcdefgh, abcd1234);
  - The following sequence of letters - passwrd, passwd, pwrd, paswd, passwd.
- Staff who suspect their password is known by others must change their password immediately.
- Staff must ensure all default passwords which are supplied by a vendor for new I.T. devices and information systems are changed at installation time.

Please refer to the school's Data Protection Policy which provides clear guidance regarding the accepted use of data in the school. The policy is available from the Principal.

Software & Electronic Media

Each user is responsible for making use of software and electronic media in accordance with the Irish *Copyright and Related Rights Act 2000* and software licensing agreements.

Policy

- Only software which has the correct and proper license may be installed and used within the school.
- Mobile and smart device application software (i.e. apps) must only be downloaded and installed on school devices where there is a valid school reason and the software can add value to the users work for the school.
- All software and electronic media developed and purchased on behalf the school remains the property of the school and must not be used, copied, distributed or borrowed without the authorisation of the school.
- The school reserves the right to remove software at any time, for reasons including but not limited:
    - non-compliance with school policies;
    - the software is not properly licensed;
    - the software is found to have a negative impact on the performance of the school network, systems or equipment.

An Approved Software List (Back of this document) is maintained by the Principal. Staff should refer to this list before downloading, accessing or using any 3rd party software in connection with school business.

IT Devices & Equipment

All I.T. devices and equipment are purchased through the agreed channels, national contract agreements or agreed ICT framework agreements.

Policy

- All I.T. devices and equipment provided by the school remain the property of the school.
- Staff must not remove or borrow school I.T. devices or equipment without the authorisation of Principal. The physical security of any school I.T. devices and equipment borrowed is the responsibility of the borrower and the I.T. devices and equipment must be returned by the borrower before they leave the employment of the school or, at the request of the Principal.
- Staff must not alter the hardware or software configuration of any school I.T. device or equipment without the prior authorisation of the school.
- Staff must take due care when using school I.T. devices and equipment and take reasonable steps to ensure that no damage is caused to the I.T. device or equipment. They must not use I.T. devices and equipment (either in a school facility, while traveling or at home) if they have reason to believe it is dangerous to themselves or others.
- Staff must report all damaged, lost or stolen school I.T. devices and equipment to the Principal.
- Old and obsolete school I.T. devices and equipment will be recycled in accordance with the requirements of the European Waste Electrical and Electronic Equipment (WEEE) Directive.
- Staff must notify the school of any old I.T. devices and equipment and they will facilitate the collection and disposal of the devices and equipment.
- The school reserves the right to remove any I.T. devices and equipment from the network at any time, for reasons including but not limited to (1) noncompliance with school policies, (2) the I.T. device or equipment does not meet approved specification and standard, or (3) the I.T. device or equipment is deemed to be interfering with the operation of the network.

I.T. Equipment must be returned by staff before they leave the employment of the school. In addition, the school will then disable access to school software applications, networks etc.

Computer & Peripherals

Staff should be conscious of the use of computers and peripherals in the day to day operation of the school.

Policy

- Staff should operate a clear screen policy and log off or 'lock' their school computer (using *Ctrl+Alt+Delete* keys) when they have to leave it unattended for any period of time and at the end of the each working day.
- Where practical staff should operate a clear desk policy and clear their desks of all confidential and restricted information (irrespective of the format) at the end of each working day or when leaving their workplace for a major part of the day,
- Where possible, printers, scanners and photocopiers which are used to regularly print, scan or copy confidential or restricted information should be located within areas which are not accessible by the general public.
- Confidential and restricted information, when printed, scanned or copied should where practical be collected from the printer, scanner or photocopier immediately.

The Child Trafficking And Pornography Act 1998

The sharing or storing of explicit images is an unacceptable and absolute prohibited behaviour, with serious consequences and sanctions for those involved.

Policy

- The school has a duty of care to students under health and safety legislation as well as the Child Trafficking And Pornography Act 1998.
- Every child including students of the school has a right to an effective learning environment in school at all times free from risk of exploitation.
- The Board of Management reserve the right to contact the Gardai should there be a strong suspicion of a member of staff acting illegally using school technologies.

Mobile Computer Devices & Smart Devices

Staff must ensure that school devices and smart devices provided to them are protected at all times.

Requirements

- Staff must ensure that school laptops, mobile computer devices and smart devices provided to them are protected at all times. They 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 smart devices must only be issued to staff who have signed a copy of the Acceptable Use Agreement (In appendix).
- All school smart devices must be registered with the IT post holder so that they can be routed through the school network infrastructure and managed securely.
- School Laptops, mobile computer devices and smart devices must be password protected in accordance with the user accounts and password policy on page 8.
- 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 desktop, mobile computer devices and smart devices must have a password / pin code / swipe gesture to gain access.
- When traveling by car, school laptops, mobile computer devices and smart devices should be stored securely out of sight when not in use. Avoid leaving the devices unattended in the boot of a car overnight.
- The use of school smart devices within a car must at all times be made in accordance with the Road Traffic Act 2006.
- When traveling by taxi, train or plane school laptops, mobile computer devices and smart devices should be kept close to hand at all times. Avoid placing the devices in locations where they could easily be forgotten or left behind (i.e. in overhead racks or boots of taxis).
- When using a school laptop, mobile computer devices or smart device in a public place staff need to take precautions to ensure the information on the device screen cannot be viewed by others.
- Staff must ensure that all school laptops, mobile computer devices and smart devices provided to them are not accessed (including internet access) by persons who are not school Staff (i.e. friends, family members and others etc).

Remote access connections to the school network from a school laptop, mobile computer devices or smart device must be made in accordance with the Work at Home Policy.

Access To School Network

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

Policy

- Access rights and privileges to the school network domains and network resources will be allocated based on the specific requirement of the member of staff.
- Access to school network domains will generally be controlled by the use of individual user access account's.
- Where there is a need and with the approval of the Board of Management through the Principal, third party commercial service providers may request and be granted local access (on-site) and/or remote access to the school network domains and information systems.
- Staff must not:
    - Disconnect any school I.T. devices, equipment or removable storage devices to or from a school network domain without the prior authorisation of the Principal.
    - Connect any school I.T. devices and equipment, laptop or smart device to an external network without the prior authorisation of the Principal.
    - Connect any I.T. 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 Principal

All non-school staff given access to local server / comms rooms or other areas housing school network servers and/or network and data communication equipment must be accompanied by an authorized school staff member throughout their visit.

Information Storage

For security and legal reasons, the school's preferred position is that:

Policy

- All school confidential or restricted information is stored on a school network server (internal), school supplied cloud (G-Suite for Education) or school supplied information management system (E-Portal).
- Confidential or restricted information stored on a school network server which is not stored as part of a school information system must be held within a secure folder which is only accessible by authorised staff.
- School network servers are reserved for the hosting/storage of school business related systems and information only. Staff must store all non-school personal information (i.e. information which is of a personal nature and belongs to the user and not the school) on their local school computer device.
- Staff are not permitted to store confidential or restricted information i.e. personal data on a personal USB Stick, Hard Drive or Personal Cloud i.e. Dropbox, Google Drive, Box etc.
- Under no circumstance should USB memory sticks (encrypted or otherwise) be used to transfer or store school information systems, confidential information or restricted information.
- Removable storage devices and school approved encrypted USB memory sticks except those used for backup purposes must not be used for the long-term storage of confidential or personal information.
- 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 practical. When the transfer is complete the photographic, video or audio recording on the recording device should be deleted.

Appropriate technical and organizational measures will be implemented to protect data stored on school devices. This may include hard drive encryption and 2 step verification.

Information Disposal

Confidential and restricted information must be securely deleted when it is no longer required.

Policy

- All traces of confidential and restricted information must be purged from old school computers, smart devices, mobile computer devices, mobile phone devices and removable storage devices before they are reused within the school or recycled.
- The simple deletion or formatting of information stored on a device is not sufficient to remove all traces of the information. The information must be purged by either (1) using special sanitation software to overwrite the information a number of times, or (2) the hard disk must be degaussed (i.e. information is permanently purged using a powerful magnet) or (3) the physical destruction of the media (i.e. hard disk, magnetic tape, video & audio tapes, CD/DVD's, floppy disks etc) the information is stored on.
- Photocopiers and scanners which are fitted with hard disks must be purged of all confidential and personal data before they are disposed of or returned to the vendor.
- Computers and other I.T. equipment which are leased from third parties must be purged of all confidential and personal data before being returned to the third-party leasing company.

Where the disposal of old school computer equipment and removable storage devices is outsourced to a commercial service provider the commercial service provider must:

- Ensure the operation of purging the computer equipment of all confidential and restricted information and the destruction of the media (i.e. hard disk, magnetic tape, video & audio tapes, CD/DVD's, floppy disks etc) is carried out on-site at a school facility before the equipment is taken off-site to a licensed WEEE recycling facility within Ireland.
- Provide the school with a certificate of disposal / destruction for all the equipment that was disposed of / destroyed by them.

Working From Home

School business is normally conducted in person within the school building. In exceptional circumstances, and at the discretion of the Board of Management, remote working will be facilitated.

Policy

- Staff who are authorised by the school to work from home must take all reasonable measures to ensure that access to school software applications are kept secure and are protected against unauthorised access, damage, loss.
- All work carried out by them on behalf of the school while working at home is done so using the Core Technologies on the "Approved Technologies" List in Appendix 1.
- The storage of data is restricted to G-Suite for Education & E-Portal and not any other platform which is their personal property or the personal property of another household member;
- All school supplied software used by them to work from home should be password protected in accordance with this policy.
- All confidential and restricted information which is accessed by them must be kept secure and confidential at all times;
- All school software and information provided to them are not accessed (including internet access) by members of their family, other household members or visitors;
- All old printouts and other paper-based records that contain confidential or restricted information are shredded or disposed of securely and are not disposed along with their ordinary household rubbish;
- School Data on Personal Devices
    - When working from a personal device please ensure that you work from within the browser when working with personal data i.e. Word Online, Excel Online, E-Portal etc.
    - If you inadvertently download a document containing personal data, please ensure that you delete the document from your hard drive.
    - Never safe or cache the username / password on your personal device.
    - Once you are back at school, conduct a search of all devices to ensure that personal data is deleted / moved to the school cloud.

Protocol for Live Classes

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

Policy

- Each teacher and student will be assigned an individual account name and password set which they can use to access a particular IT 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 behave as they would do in a normal classroom setting.
- Students are expected to conduct themselves with respect for both the teacher and their classmates.
- Escalation Policy – In the event of a student becoming disruptive in class the following escalation policy will be followed:
    - Student will be instructed to behave;
    - If the student does not comply, the student will be muted by the teacher to avoid further disruption;
    - If the disruption persists, the student's video will be turned off by the teacher;
    - Finally, if disruption persists the student will be removed from the online class and reported to the Principal. At this point the school's code of behaviour will then apply.

When broadcasting classes on Zoom 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;

Protocol for Live Meetings

Should the school need to revert to online meetings for both staff and student meetings in light of Covid-19.

Policy

- Each teacher will be assigned an individual account name and password set which they can use to access a particular IT 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.
- Online Meetings i.e. Department meetings, meetings with the Principal / Deputy Principal are permitted to take place on Zoom exclusively.
- Staff consider all online meetings as potentially sensitive and ensure that they are located in a quiet room where others cannot overhear the discussion.
- The use of WhatsApp is not permitted for communications involving personal data.
- Chat Function should not be used to share data with colleagues.
- Staff should password protect any documents containing personal data and send this information only to those who need it via email.
- Minutes of meetings should be saved to the user's Google Drive Account and never locally to a personal storage device.

When teachers are conducting one to one sessions with students i.e. regarding Counselling, SEN, Disciplinary matters. The following protocol applies:

- School supplied G-Suite for Education Accounts should be used to set up and conduct the meeting;
- Video may be used and at either party's discretion may be turned off.
- The meeting shall not be recorded.
- At any stage, either party can end the meeting with or without notice.
- If a student abruptly ends the meeting, the staff member is required to prepare a short report detailing the topic of discussion, matters raised etc. This report must be sent to the Principal and Deputy Principal within 24 hours of the meeting taking place.
- Where staff take notes, it is there responsibility to keep this data safe and secure.

Periods of Absence

Staff should be conscious of ensuring school business can be maintained in their absence.

Policy

- During planned periods of absence such as maternity / paternity leave, career breaks, holidays, on training courses or working off-site for an extended period of time, staff should ensure wherever possible that the Principal or colleagues have access to important school business related documents and emails stored on their computer so that there is no delay in dealing with matters that are due to arise.
- Staff may adopt practices that ensures data / files can be easily accessed should the need arise i.e. Storing important data on a central folder on the One Drive, copying appropriate persons on emails, maintaining a filing system that is accessed by dedicated and approved keyholders etc.

Staff Leaving

Staff should be conscious of their responsibilities when leaving the school.

Policy

- Staff must return all school devices and accessories (where supplied), information (i.e. documents, files, important email messages etc) and other important items (e.g. swipe cards, keys) to the Principal before they leave the employment of the school.
- The Principal must contact the ICT Postholder to ensure that the information system and network access accounts belonging to staff leaving the employment of the school are revoked immediately once they leave the organization.
- Staff leaving the employment of the school should also ensure they remove or delete all non-school personal information & email messages (i.e. information / email messages which are of a personal nature and belong to the user and not the school) from the devices used by them i.e. computer equipment before they leave as it may not be possible to get a copy of this data once they have left the school.

Unacceptable Use

The following list should not be seen as exhaustive. The school has the final decision on deciding what constitutes excessive personal use. The school will refer any use of its I.T. resources for illegal activities to the Gardai.

Policy

- For excessive personal use;
- For commercial activities, such as running any sort of private business, advertising or performing work for personal gain or profit;
- For political activities, such as promoting a political party / movement, or a candidate for political office, or campaigning for or against government decisions;
- To knowingly misrepresent the school;
- To transmit confidential or restricted information outside the school unless the information has been encrypted and transmission has been authorised by the Principal;
- To store or transfer confidential or restricted information(encrypted or otherwise) onto a USB memory stick;
- To enter into contractual agreements inappropriately (i.e. without authorisation or where another form of agreement is required);
- To create, view, download, host or transmit material (other than staff who are authorised by the school to access such material for research etc.) 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;
- For any activity that would infringe intellectual property rights (e.g. unlicensed 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;
- For any activity that would deliberately cause the corruption or destruction of data belonging to the school or others;
- For any activity that would intentionally waste the school's resources (e.g. staff time and IT resources);
- For any activity that would intentionally compromise the security of the school's IT resources, including the confidentiality and integrity of information and availability of IT resources (e.g. by deliberately or carelessly causing computer virus and malicious software infection);
- For the installation and use of software or hardware tools which could be used to probe or break the school I.T. security controls;
- For the installation and use of software or hardware tools which could be used for the unauthorised monitoring of electronic communications within the school or elsewhere;
- To gain access to information systems or information belonging to the school or others which you are not authorized to use;

Student's Use Of Technology

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:

General Accepted Use

- Internet sessions will always be supervised by a teacher.
- Filtering software and/or equivalent systems (commonly known as "Nanny Software") will be used in order to minimise the risk of exposure to inappropriate material.
- The school will regularly monitor students' Internet usage.
- Students and teachers will be provided with training in the area of Internet safety.
- Uploading and downloading of non-approved software will not be permitted.
- Virus protection software will be used and updated on a regular basis.
- The use of personal memory sticks, CD-ROMs, or other digital storage media in school requires a teacher's permission. However, the transfer of personal data is prohibited through these devices.
- Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.

Internet Use

- Students will not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Students will report accidental accessing of inappropriate materials in accordance with school procedures.
- Students will use the Internet for educational purposes only.
- Students will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).
- Students will never disclose or publicise personal information.
- Downloading by students of materials or images not relevant to their studies is in direct breach of the school's acceptable use policy.
- Students will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.

Email Use

- Students will use approved class email accounts under supervision by or permission from a teacher.
- Children's use of email is facilitated strictly in an educational context and access to personal email and/or social networking accounts is prohibited.
- Online tasks that involve sending and receiving email (e.g. with partner schools, educational email tasks) will be teacher-led. The class teacher will set up one email address for the class. Only the teacher will know the password to such email accounts. Emails will be opened and read by the teacher before being shared with the class. All emails will be reviewed by the teacher prior to sending.
- 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.

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.
- Discussions online will be done with dignity and respect.
- 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.

School Website

- 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.
- The school will endeavour to use digital photographs, audio or video clips of focusing on group activities. Content focusing will not be published on the school website without the parental permission. 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.

Use of Social Media

Unacceptable Uses of Social Media sites and the Consequences of that Use
All members of the school community are responsible for their own behaviour when communicating with social media and will be held accountable for the content of their communications that they post on social media locations.

Examples of Unacceptable Use of Social Media

- Sending or posting discriminatory, harassing, negative comments, threatening messages or images that may cause harm to any member of the school community.
- Forwarding, 'Liking' or commenting on material that is likely to cause offence or hurt to a third party.
- Sending or posting messages or material that could damage the school's image or a person's reputation.
- Creating a fake profile that impersonates any other member of the school community.
- Sending or posting material that is confidential to the school.
- Participating in the viewing or exchanging of inappropriate images or obscene material.

While all cases involving the inappropriate use of social media will be dealt with on an individual basis, the school and its Board of Management considers the above to be serious breaches of our Code of Behaviour. Disciplinary action will be taken in the case of inappropriate use of social media tools. This list is not exhaustive.

Sanctions for Social Media Policy Infringements
For pupils, Infringements of this policy may have disciplinary repercussions, including (but not exclusively):

- Suspension of computer privileges in school
- Confiscation of devices if found on school grounds or on school related activities
- Notification to parents
- Suspension from school and school- related activities
- Exclusion
- Legal action and/or prosecution

For parents, infringements of this policy will be referred to the Gardaí or relevant agencies where deemed appropriate by the Board of Management.

Please note that some inappropriate behaviour may be the subject of mandatory reporting to the relevant authorities or agencies.

Assistive Technologies

- Where laptops are provided for student use i.e. assistive technologies, each laptop will be configured for student use. Parental Controls will be enabled and student accounts are granted restricted access and control.
- Student laptops will have Microsoft Family Safety or equivalent installed, which provides the school with weekly reports of student online activity on each laptop.
- Students will be denied access to internet browsers such as Google Chrome and Internet Explorer etc. and where deemed necessary an age appropriate and internet-safe browser (Kudzu or equivalent) will be installed as the default student browser on each laptop.
- In the event that a web browser is accessed (or granted access), laptops will be configured to block (and subsequently notify the school) of any attempts by users to access content deemed to be inappropriate for students.
- Students are allowed to connect to wireless networks on their school supplied laptops / tablets. This will assist them with use while at home. Acceptable Use Section of this policy still applies while off the school premises. Students experiencing difficulty with internet access at home should contact their Internet Service Provider (ISP).
- Students may be selected at random to provide their school supplied laptop / tablet for inspection. If a student's device is requested for an inspection, students must unlock the device.
- When students are not using their school supplied tablets / laptops, they should be stored safely.

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. Only used with the permission of the class teacher.

Cyber Bullying

- This refers to bullying carried out using the internet, mobile phone or other technological devices. Cyberbullying can take many forms including texts, Instant messaging, Sending nasty, mean or threatening messages, emails, photos or video clips, Silent phone calls, Putting up nasty posts or pictures online on social media platforms, message boards, websites or chat rooms, Pretending to be someone else in a chatroom, message board or text message and saying hurtful things, Accessing someone's account to torment or harass him or her. Misuse of any other medium/technological device. Harassing, flaming, denigrating, impersonating, outing, tricking, excluding and cyber-stalking are all examples of cyber-bullying.
- Cyberbullying will not be tolerated. As all pupils and parents alike have signed the School A.U.P, let them understand that, as with any case of bullying, the School takes these cyberbullying threats very seriously and will act appropriately to prevent them. In a case of cyberbullying, the school will follow the Anti-bullying policy. Note that any one incident online may be treated as bullying and that it **is not necessary** that there be *unwanted negative behaviour, verbal, psychological or physical conducted, by an individual or group against another person (or persons) and which is* ***repeated over time.*** The School wil implement the Anti-Bullying Policy when dealing with pupils who have taken part in cyberbullying (or any type of bullying) on other pupils before, during or after school hours (If it affects school life).

Teacher's Use Of Technology

Various technologies are provided by the school and made available to staff to further their professional development and the education of the students in the school. Access to the school's supplied technologies is a privilege and not a right.

Any staff member or visitor who abuses this privilege will be immediately excluded from accessing and using these technologies.

Email Use

- Teachers will use approved school email accounts for all communications.
- Teacher's use of email is facilitated strictly in an educational context and access to personal email and/or social networking accounts is prohibited.
- Staff must not send any emails that are likely to cause distress or any material which is offensive, indecent, obscene, menacing, or in any way unlawful.
- Staff must not use the school network, or E-Portal online software to send messages or emails to any user who does not wish to receive them.
- The school network must not be used to send or distribute unsolicited commercial mail, commonly known as 'spam', in bulk or individually.
- Staff, as senders of emails, must not use false mail headers or alter the headers of mail messages in such a way as to conceal the identity of the sender.
- Where emails and attachments contain sensitive personal information, staff are required to encrypt these emails. Attachments including sensitive personal information should be password protected i.e. ensuring only the recipient(s) with a password can open and access the contents of the email.
- Staff will not save copies of personal data to their own personal computers, phones, tablets, USB sticks, Hard Drives;
- 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.

Use of E-Portal

- In order to protect the information that is accessible on E-Portal, users must not divulge their logon details to third parties. Any concerns or queries must be forwarded and dealt by an Administrator with rights on the E-Portal system.
- Where enabled, 2 Step Verification will be used to verify staff logins.

Use of Social Media

Personal use of Social Media

The Code of Professional Conduct published by the Teaching Council governs the use of Social Media sites by staff. Staff are encouraged to use the privacy settings on social media sites/apps and to keep updated on developments on privacy restrictions. Staff are expected to exercise sound judgement and maintain the highest professional standards while using social media in the school.

Unacceptable Uses of Social Media sites and the Consequences of that Use

All members of the school community are responsible for their own behaviour when communicating with social media and will be held accountable for the content of their communications that they post on social media locations.

Examples of Unacceptable Use of Social Media

- Sending or posting discriminatory, harassing, negative comments, threatening messages or images that may cause harm to any member of the school community.
- Forwarding, 'Liking' or commenting on material that is likely to cause offence or hurt to a third party.
- Sending or posting messages or material that could damage the school's image or a person's reputation.
- Creating a fake profile that impersonates any other member of the school community.
- Sending or posting material that is confidential to the school.
- Participating in the viewing or exchanging of inappropriate images or obscene material.

While all cases involving the inappropriate use of social media will be dealt with on an individual basis, the school and its Board of Management considers the above to be serious breaches of our Code of Behaviour. Disciplinary action will be taken in the case of inappropriate use of social media tools. This list is not exhaustive.

For teachers, infringements of this policy will be dealt with in accordance with the Code of Professional Conduct.

Please note that some inappropriate behaviour may be the subject of mandatory reporting to the relevant authorities or agencies.

Use of Networks & Internet

- Staff must not use the service for the transmission of illegal material. The user agrees to refrain from sending or receiving any materials which may be deemed to be offensive, abusive, indecent, hard-core or paedophile pornography, defamatory, obscene, menacing or otherwise as prohibited by current and future statutes in force.
- Staff agree to refrain from sending or receiving any material, which may be in breach of copyright (including intellectual property rights), confidence, privacy, or other rights.
- If you are in any doubt as the legality of what you are doing, or propose to do, you should either seek advice from the Principal or cease that usage.
- Student's work should never be shared on social networking sites or websites other than the school website. Sharing or making references to a student's work, especially if it could undermine the student, is not acceptable.
- Staff should be aware that the storage, distribution of, or transmission of illegal materials may lead to investigation and possible prosecution by the authorities.
- Staff may not gain or attempt to gain unauthorised access to any computer for any purpose.
- Staff must not send data via the internet using forged addresses or data which is deliberately designed to adversely affect remote machines (including but not limited to denial of service, ping storm, Trojans, worms, and viruses).
- Staff must not participate in the sending of unsolicited commercial or bulk email, commonly referred to as 'spam'.
- Staff are prohibited from running 'port scanning' or other software intended to probe, scan, test vulnerability of or access remote systems or networks except in circumstances where the remote user has given express permission for this to be done.
- Staff may not divulge their computer network passwords to third parties and must take all reasonable steps to ensure that such information remains confidential.
- Access to the computer network should only be made using the authorised logon name and password.
- The use of USB Sticks / Hard Drives for storage of personal data is prohibited.
- The use of the network to access and/or store inappropriate materials such as pornographic, racist, or offensive material is forbidden.
- In the interest of protecting the network from potential virus activity, the downloading of programs, games, screensavers, and wallpapers from the internet or uploading the same from disc or CD-ROM may only be carried out by the ICT Coordinator. This does not prevent Staff from using images taken and/or saved by them to set their desktop backgrounds.
- Use of the computing facilities for personal financial gain, gambling, political purposes, or advertising is forbidden.
- Copyright of material must be respected, particularly with regard to the download and use of protected images for further use.

Appendix 1: Approved Technologies For Use

Approved Technologies are technologies that the school has approved for use by relevant staff in their day to day work in the school. From time to time this list may be updated to reflect changes in how we do things or changing circumstances outside our control.

Core Software Applications (Teaching Staff)

- E-Portal;
- Facility;
- G-Suite for Education;
- Website;
- Microsoft Office;

Core Software Applications (Administration)

- PPOD;
- ESI Net;
- Sage;
- Thesaurus;

Board of Management Approval

Board of Management of Coláiste Phádraig, approved the revised Acceptable Use Policy on _____.

Signed: _____
Chairperson