COLÁISTE NA TOIRBHIRTE ICT POLICY

ICT Acceptable Use

Colaiste na Toirbhirte is committed to ensure that all users including students, staff and parents will benefit from learning opportunities offered by the school's Information Technology (IT) system in a safe, effective and appropriate manner. The policy is also mindful of the need to bring the key components of the school's mission statement into the daily lives of all who work in the school.

The Aims of This Policy:

- To promote the professional, ethical, lawful and productive use of IT.
- To define and prohibit unacceptable use of IT
- To educate users about their IT Security responsibilities
- To promote practices to ensure appropriate confidentiality and non-disclosure of the School's sensitive information
- To describe where, when and why monitoring may take place

If the school's IT ACCEPTABLE USE POLICY is not adhered to, access to the school's IT system may be withdrawn and appropriate disciplinary actions will be imposed in accordance with established procedures.

Section 1

1. General Principles

Things to know

ⓘ Information Security is everybody's responsibility.
ⓘ The School's IT systems are provided for educational use
ⓘ Use of any of the school's IT systems for personal reasons (including e-mail and the web) is only permitted in accordance with the guidance in this policy.
ⓘ The School reserves the right to monitor any aspect of its information systems in order to protect its lawful interests, prevent and/or detect crime, discriminatory and harassing behaviour. Information gathered from such monitoring may be used to instigate or support disciplinary proceedings and may be disclosed to the Gardaí or any other investigatory body.
ⓘ This policy refers in several places to things that "Others may find offensive". These include but are not limited to:-

- Pornographic or sexually explicit material
- Discriminatory and harassing behaviour

ⓘ The School will deal with incidents that take place outside the school that impact on the wellbeing of students or staff under this policy and associated policies. In such cases the School will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of school and impose the appropriate sanctions.

ⓘ The School implements the following strategies on promoting safer use of the internet:

- Education for students in internet safety as part of the Wellbeing curriculum.
- The School participates in Safer Internet Day activities
- Teachers will be provided with CPD opportunities in the area of internet safety.
- Internet safety advice and support are provided to students through our IT class and visit by Garda Internet Safety Officer.

ⓘ Should serious online safety incidents take place, the Designated Liaison Person (DLP) for child protection Mary O'Donovan, should be informed

Things to do

☑ Treat others with respect at all times.
☑ Respect the right to privacy of all members of the school community.
☑ Respect copyright and acknowledge creators when using online content and resources.
☑ Exercise care and common sense in your use of information technology.

Things not to do

☒ Anything illegal.

☒ Anything that contravenes this policy.

☒ Anything that will harm the reputation of the School.

☒ Anything that contravenes the School's Dignity in the Workplace, Code of Behaviour and Antibullying Policies.

2. Desktop Computers

Things to know

ⓘ Desktop computers are the property of the School and have been prepared by the IT department for use on the School network.

ⓘ Authorised software is installed on your computer and you are not allowed to install anything on your own.

ⓘ Data saved to local C: drives will not be backed up, and will be lost if the computer breaks, gets stolen or is replaced.
However data saved to the D drive (school server) is backed up to a secure cloud storage service and it is recommended to save your data to the school server.

ⓘ The School may at any time and without prior notice:-

- Audit the computers to ensure compliance with policy.

Things to do

☑ Log off from any workstation (CTRL+ALT+DEL) once you are finished using it.

☑ Save data to your personal One Drive (Office 365 account).

☑ Ensure that files received from anywhere outside the School are virus checked before you open them. This includes files on CD or USB drive. If in doubt, ask the IT Co-ordinator to scan it for you.

☑ **If you suspect a computer you are using may have a virus, leave the computer on, unplug the network cable and call the IT Co-ordinator.**

☑ Turn any PC and monitor off at night to save energy unless there is a specific reason to leave it on.

Things not to do

☒ Do not allow anyone else to use a computer while you are logged in.

☒ **Never install software on your computer**. This should only be done by the IT Co-ordinator or IT Team. Things that you should never attempt to install include but are not limited to:-

- Screen savers and games, music download software
- Utilities that claim to remove spyware or viruses
- Applications that download torrents such a showbox, popcorn, moviebox etc

☒ Do not disable or uninstall any of the software that is installed on your computer

3. Portable Computers

ⓘ The term 'portable computer' covers any school-owned mobile computing device including:-

- Laptop or tablets (iPads)

ⓘ All PCs, laptops and iPads are the property of the School and have been prepared by the IT department for use on the School network. **They cannot be removed from school site.**

ⓘ The School may at any time and without prior notice:-

- Audit the computers to ensure compliance with policy

ⓘ You are taking full responsibility for everything done on your portable computer.

ⓘ You are responsible for the care and safe storage of any computer equipment that has been issued to you.

Things not to do

☒ **Never install software on your computer**. This should only be done by the IT Co-ordinator or IT Team. Things that you should never attempt to install include but are not limited to:-
- o Screen savers and games, music download software
- o Utilities that claim to remove spyware or viruses
- o News readers or ticker-tape services
- o Applications that download torrents such a showbox, popcorn, moviebox etc.

☒ Do not allow family, friends or anybody else to use the computer.

☒ Do not allow visitors (guest speakers etc.) to connect their laptops to the School's network before getting the approval from IT Department

4. Email - Office 365

Things to know

ⓘ The School's e-mail systems are provided for school use. Reasonable personal use is permitted provided it is lawful, ethical and takes place during authorised breaks.

ⓘ The School reserves the right to monitor all e-mail to ensure compliance with policy

ⓘ E-mail is not a secure method of communication. Once a message is sent you have no further control over who reads it.

ⓘ E-mail is admissible evidence in any legal proceedings and carries the same weight as a letter on school headed paper.

ⓘ School email accounts may not be used to register for online services such as social networking services, games and purchasing.

ⓘ Students will use approved email accounts only under supervision by or permission from a teacher.

Things to do

☑ Use the same care when drafting an e-mail message as you would when writing a letter or memo on school headed paper.

☑ Make sure that your message is concise, relevant and sent only to the people that need to read it.

☑ Check your e-mails every day and clear out old and unwanted messages from your mailbox.

☑ Return any wrongly delivered message to the sender. If it contains confidential information it should not be disclosed or used in any way.

☑ Immediately report to the Principal the receipt of any communication that makes you feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and do not respond to any such communication.

Things not to do

☒ **Never open an attachment that you were not expecting, even if you know the sender.**

☒ Do not use personal emails accounts for any school communication or business.

☒ Do not use e-mail to send sensitive or confidential information.

☒ Do not send or forward anything that:-
- o Is illegal, obscene, others may find offensive, may be defamatory or harassing
- o Is covered by a copyright (pictures, movies, music, others)

☒ Do not circulate non school-related material. This includes but is not limited to:-
- o Chain letters, , virus warnings, software

☒ Never use e-mail to rebuke, criticise or complain about somebody. You may say something that you regret, and the record will be permanent.

☒ Never supply banking or payment details in response to an e-mail message. This is a wellknown method of fraud. Your bank will never request security details by e-mail.

5. Your Password

Things to know

ⓘ Your password is confidential and it is not transferable to anyone else.
ⓘ The password requirements for Office 365 must be at least 8 characters long and contain a capital, a lowercase and a number.
ⓘ The access rights associated with your office 365 account may be changed or revoked should your status as an employee or student change/terminate.

Things to do

☑ Set a password or phrase. Make it as secure as you can by using some or all of the following techniques:-

- Use two unrelated words or a short phrase
- Include at least one number
- Include at least one upper case character
- User name can't be part of your password
- Password has to be at least 8 characters long

☑ Change your password if you suspect that someone else may know it.

Things not to do

☒ Do not disclose your password to anyone.
☒ Do not use anyone else's password.
☒ Do not write down your password. You need to remember it.

6. Web Access (including wifi access) and content filtering

Things to know

ⓘ Web access is provided for school use. Reasonable personal use is permitted provided it is lawful, ethical and takes place during authorised breaks.
ⓘ The School has chosen to implement two levels of content filtering:-

1. **Level 3 content filtering on the schools broadband network, for <u>student access</u>, which aligns to NCTE guidelines:**

- **This level allows access to millions of websites but blocks access to You tube, blogs and social networking sites like Facebook.**

The School wifi network is aligned to Level 3 content filtering .

IMPORTANT: Staff and those guests to school authorised by school management only have access to the wifi password. A staff member should never divulge this password to a student. If this occurs the password will immediately have to be changed.

2. **Staff PCs in classrooms are on a separate network where there are less restrictions. Please refer to Social media guidelines and acceptable usage policy below for more information on staff responsibilities with regard to internet access.**

ⓘ Any person taking steps to by-pass the content filter by any means may be subject to disciplinary action.

ⓘ All web access can be monitored by the school to ensure compliance with the policy. Users that choose to make personal use of the schools IT system do so in acceptance of the monitoring measures outlined in this policy.

Things to do

☑ Use the school's internet connection for educational and career development activities only.
☑ Report accidental accessing of inappropriate materials to the teacher or IT Co-ordinator.
☑ Sites that are blocked usually ask you to click on a particular section to fill in a request to have the site reviewed by the NCTE as appropriate for teaching purposes. Please use this method of getting sites unblocked as the IT Co-ordinator has no control over unblocking sites.
☑ **If you suspect a computer you are using may have a virus or spy-ware infection, leave**

the computer on, unplug the network cable and call the IT Co-ordinator.

Things not to do

☒ Never divulge wifi password to students

☒ Do not View or download anything that others may find offensive, illegal, obscene and defamatory.

☒ Do not upload or download large files that results in heavy network traffic and affect performance for other users.

☒ Do not download anything that is likely to be covered by copyright. This includes, but is not limited to:-

- Music, Pictures, Software and Movies

☒ Do not visit the "high-risk" site categories. Although their content appears to be free, it is often funded by installing spyware on your computer.

☒ Do not download any attachments using personal web based mailboxes (Yahoo, Hotmail etc.) as it is not monitored by the School security software.

☒ Do not listen to the radio stations through internet as the radio stream consumes too many resources in the network that will affect performance.

7a) Social Media and Cyberbullying

Things to know

Social media refers to social and professional networking platforms such as Facebook, Twitter, Whats App, Instagram , message boards and other similar online facilities.
It is the parent/guardian's responsibility to monitor student's use of social media outside of school hours.

ⓘ The use of instant messaging services and apps including Snapchat, WhatsApp, GChat etc. is **strictly prohibited for students** on the School network.

ⓘ The use of Blogs such as Word Press, Tumblr etc. is allowed with express permission from teaching staff.

ⓘ The use of video sites such as YouTube is allowed with express permission from the teaching staff.

ⓘ **Engaging in online activities with the intention to harm, harass, or embarrass another student or member of staff is an unacceptable and absolutely prohibited behaviour, with serious consequences and sanctions for those involved.**

ⓘ **Isolated or once-off incidents of intentional negative behaviour, including a once-off offensive or hurtful text message or private messaging, do not fall within the definition of bullying and will be dealt with, as appropriate, in accordance with the school's code of behaviour.**

The school will work closely with parents/guardians in order to resolve any issues of bullying that may arise on social media which may impact on a student's well-being in school.

Things to do - students

☑ Treat others with respect at all times.

☑ Report any incident of cyber bullying to the school

Things not to do - students

☒ Do not use social media in any way to harass, insult, abuse or defame students, their family members, staff, other members of the school community.

☒ Do not discuss personal information about students, staff and other members of the school community on social media.

☒ Do not represent your personal views as those of being Coláiste na Toirbhirte on any social medium.

7b) Social Media Guidelines and Acceptable Usage Policy - staff

Things to know

Staff are at all times prohibited from using or publishing information on social media which has the potential to negatively impact on the School community or damage the reputation of the school.

Staff Acceptable Usage Policy

1. **Social Media usage in the course of employment which relates to school business/matters**

Things to do

☑ Seek permission from Principal before setting up a site or profile relating to school business.

Things to know - staff

A permitted employee is responsible for his/her social media usage and must comply with the terms and conditions of the relevant social media platform

Things not to do – staff

☒ **Staff are at all times prohibited from using or publishing information on social media which has the potential to negatively impact on the School community or damage the reputation of the school.**

☒ **Employees must never reveal any private or confidential information relating to the School community.**

☒ **Employees must never create, publish, download or communicate material that could reasonably be regarded as defamatory, inappropriate, discriminatory, offensive, hostile, pornographic, damaging to the School's reputation or referring to a third person without their permission.**

2. **Personal Social Media Usage**

   Personal profiles are not to be used to conduct school business or to communicate with students/parents.

   Online interaction with management, other employees and/or school contacts should be appropriate and professional in nature.

   Employees must not use the official school E-mail address when participating in personal social media that is not related to the employee's job

   Personal use of social media must not occur during working time but is restricted to break times at work.

   Employees are personally responsible for their posts and actions on social media

Things to do

☑ **Employees should exercise sound judgement, common sense and respect when participating in social media**

☑ **When an employee chooses to identify him/herself on social media as an employee of the school it must be made clear that their communications do not represent the School, its ethos, position, opinions or views**

☑ **Staff should immediately report to the DLP any inappropriate or unacceptable social media activity concerning the School/School community**

Things not to do - staff

☒ **Staff are at all times prohibited from using or publishing information on social media which has the potential to negatively impact on the School community or damage the reputation of the school.**

.

8. Responsible use of Resources

Things to know

ⓘ Implementing the small changes described on this page can make a big difference to the School's costs, and also to the environment.

.

Things to do

☑ Shut your computer down at the end of your working day rather than just logging off.

☑ Turn off your monitor before you leave rather than leaving it in standby

☑ If you have a workgroup printer or copier in your area, establish a routine with your colleagues so that it gets turned off at night and back on in the morning (15 tonnes per device).

☑ Unplug or switch off phone, PDA or portable device chargers when they are not in use.

Things not to do

☒ Do not turn off computer equipment on behalf of someone else. There may be a good reason why it has been left on.

☒ Do not use USB storage device that is not antivirus protected.

9. Monitoring

The School owns its IT systems. It reserves the right to monitor any school system at any time. Monitoring of any device/system can be done by or on request from the Principal, Deputy Principal, IT co-ordinator and IT support company associated with the school.

Monitoring of systems is carried out by the Principal and IT Co-ordinator in order to:-

- Detect and prevent unlawful use of systems
- Detect and prevent misuse of school systems
- Maintain the effective operation of systems
- Protect the School's employees
- Protect the reputation of the School
- Protect the School from legal liability

Monitoring of the school's information systems will be conducted in accordance with the provisions of legislation in force from time to time, in particular :-

- General Data Protection Regulation (GDPR) May 2018
- Data Protection Act
- Child Trafficking and Pornography Act 1997
- Interception Act 1993
- Video Recordings Act 1989
- Teaching Council Code of Professional Conduct
- Human Rights Act 1998 and the European Convention on Human Rights (if applicable)

At the request of the Board of Management or as needed, management of the School may pass on requested data to any of the following:

- ☐ The Principal
- ☐ The Gardaí
- ☐ Other parties as required by law

10. Data Protection Responsibilities

Things to know

ⓘ You are personally responsible for ensuring the confidentiality of a student's personal data.

Things to do

☑ Log off from any workstation (CTRL+ALT+DEL) once you are finished using it.

☑ When distributing information use codes/abbreviation rather than names.

☑ Ensure Avast antivirus is running on your laptop or Desktop Computer.

☑ If Personal Data is saved to a USB drive ensure it is fully encrypted.

☑ If you process personal data (data that identifies a living individual) in the course of your work, you must do this in accordance with General Data Protection Regulation (GDPR) May 2018.

Things not to do

☒ Do not view sensitive information on the train, plane or in any public area. This provides an opportunity for onlookers.

☒ Do not allow family, friends or anybody else to use the computer which contain student information.

☒ When communicating information through email do no put names in the subject bar.

☒ Do not disclose or share any sensitive information to other people if not under the expressed authorisation of the Principal.

☒ Do not leave printed documents around the printer as they may contain confidential data.

11. Printing

Things to know

ⓘ Printers are provided for educational use only.

Things to do

☑ Be selective about what you print. Print only when necessary and only the necessary pages of a document.

☑ Double sided printing as set as a default setting on all the printers to save paper.

☑ Use a photocopier when producing a large number of copies.

☑ Keep the area around printers tidy.

Things not to do

☒ **Students cannot access printer without staff permission and should be supervised by staff member at all times during printing**

☒ Do not print to a colour printer unless colour conveys important information in your document that would be lost in black and white. A charge will apply to all student colour printing.

☒ Do not resend your print job if nothing happens. Instead, check the following:-

- o Is the print job still listed in the queue?
- o Is the printer switched on?
- o Is the printer in an error state because:-
  - There is paper jam
  - It is out of paper
  - It is out of toner or ink
- o If any of those occurs please contact ICT co-ordinator

☒ Do not leave printed documents around the printer as they may contain confidential data.

12. Disciplinary action for staff

Breach of this policy may lead to the implementation of disciplinary procedures as set out by the Teaching Council and DES
This process is described as follows:
1. Verbal warning.
2. Written warning.
3. Serious or persistent breaches may constitute gross misconduct and disciplinary procedures laid out by the teaching council and department of Education will be followed.

13. Staff Acceptance – please see form at end of this policy document

14. Disciplinary action for students

Breach of this policy may lead to the implementation of the school's Code of Behaviour.
This process is summarised as follows:
1. Verbal warning
2. Written warning
3. Withdrawal of access privileges
4. Detention
5. In extreme cases, suspension or expulsion

Information Technology (IT) Acceptable Use Policy

The School has developed a comprehensive IT acceptable usage policy. The policy can be found on the homepage of the school's website, www. presbandon.ie We ask that you look up this document online and carefully read through it before signing to confirm that you have understood this policy.

.

The aims of the policy are to:
1. Promote the professional, ethical, lawful and productive use of Coláiste na Toirbhirte's IT systems by explaining the dos and don'ts in the following areas:
a. General use
b. Desktop Computers
c. Portable devices
c. Emails (@presbandon.ie)
e. Your Password
f. Web access and content filtering
g. Social media
h. Responsible use of resources
i. Monitoring
j. Printing
k. Data Protection

2. To define unacceptable use and to state clearly how this policy will be enforced if it is breached.
3. To educate users about their IT Security responsibilities in relation to keeping passwords safe and any personal information of another person.