I.C.T. & ACCEPTABLE INTERNET USE POLICY

Presentation Secondary School,
Milltown, Co. Kerry

School Mission

Our school is a Catholic school which aspires to the full development of all its members according to Christian Principles. Every effort is made to ensure that each student develops according to his/her talents and potential: physically, spiritually, emotionally, intellectually.

We aim to develop fully integrated people who are aware of their own dignity as persons, who have Christian values, who are reliable, trustworthy, honest, truthful, caring, prayerful, devoted to duty, lovers of God and of neighbour; people who are prepared to reach out to those less fortunate than themselves.

Scope

This policy covers all members of the school community using the school's information communications technology facilities at any time.

School ICT Culture

Our aim is to help students learn how to utilise ICT in order to enhance their potential. We want students to understand that ICT is a continuously changing set of tools, which require learning, understanding and boundaries in order to use it effectively and safely.

Recognition that ICT is now universally used for social activity as well as academic and professional is also important. We aim to provide opportunities for students to learn about the risks involved in online use as well as how to stay safe online.

Aims

This policy is part of a process that integrates ICT into our school curriculum in a significant and productive way. The prime function of the policy is to provide guidelines for teachers and students to appreciate and benefit from mastering new technologies.

Curriculum

Teaching staff continue to review all teaching and learning in line with current ICT good practice.

A whole-school network supports curriculum delivery for all subject areas in providing networked resource materials, teacher-researched Internet links for student use and material for staff curriculum related professional development.

Staff

Staff have access to training in line with developments in education and ICT. Teachers are encouraged to integrate use of ICT into their subject curriculum wherever possible.

Each member of staff has access to the school's Microsoft 365 Office suite to help ensure that ICT is integrated into classroom practice.

Student Access & Multimedia Rooms

Students are facilitated with supervised use of ICT. Subject departments also ensure that students have access to ICT in their subject area via a booking system for each of two Multimedia Rooms.

It is important that ICT is used effectively to support access to the curriculum for all students.

Identified students may have access to additional resources such as laptops with specific software to support curriculum access as approved by the NCSE.
To enable the integration of ICT into everyday school life and improve its accessibility to both students and teachers the following has already been implemented in our school.

- **Microsoft 365 - Single Log-in Usernames and Passwords***:*

  From 2020 students will be issued with their own unique usernames and passwords. This will allow them to access the schools Microsoft Office 365 facility.

  They will be issued with a school email address and will be granted access to Microsoft Office tools such as Word, Excel and PowerPoint.

  Students will be encouraged to save all of their documents and work to the OneDrive associated with their Microsoft account. In line with best practice students should also keep a back-up copy of their work.

- **Share Drives: The following share drives have been created:**
  - **Class Share:** This share drive allows teachers to put work on the network for students which students can then access from any PC and save to their own account. Folders have been set up on this share drive for all subjects and teachers who wish so can create their own personal folders. Students have 'read only' access to files on this drive therefore ensuring that no information can be altered or deleted by students.
  - **Students Share:** This share drive allows students to save files to the drive that can then be accessed by other students. This has been used by e.g. Transition Year when compiling their magazines every term. **Student are advised NOT to save individual work and/or assignments to this drive as it has open access and allows for editing by any user.**

- **Seating Plan** - Students will be assigned specific sat when in the Multimedia Rooms.
  Please note – students are Not permitted to be in the Multimedia Rooms or to use school without a teacher present.

- **Fault and Repair Log** - Faults and damage must be reported to the relevant teacher who will log the issues with the ICT Coordinator. Equipment must not be moved or switched from computer to computer. Leads and cables should not be interfered with.

Data Security in School

Installing filtering or monitoring software

The importance of securing the schools infrastructure for the successful running of the school is recognised as being very important. We have a number of procedures in place that recognise this fact. Some of these are:

- **Anti-Virus Management:**
  Using and updating of Anti-Virus Software.
  We recognize that having up to date anti-virus software running on all school computers is a critical aspect of the preventative maintenance aspect of technical support. We schedule anti-virus software updates to take place outside of normal school class times.

- **Monitoring external media onto school network without it being scanned**
  All external media/devices/USBs must be scanned automatically before files are opened on the school's network**.**

INTERNET ACCEPTABLE USE POLICY

FOR ACCESS TO COMPUTER AND
INTERNET FACILITIES

The aim of this Acceptable Use Policy (AUP) is to ensure that students will benefit from learning opportunities offered by the school's IT resources in a safe and effective manner.

Internet use and access is considered a school resource and privilege. Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions will be imposed. The school will employ a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

General

- All students require permission from a teacher to use the Internet.
- Internet sessions will always be supervised by a teacher.
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material.
- The supervising teacher will monitor students' internet usage.
- Students will be made aware of internet safety issues by their teachers.
- 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 USB memory drives with school equipment requires a teacher's permission.
- Students must not use, publish or upload images/photos/comments of/about other students or staff without specific consent from the individual(s) concerned.
- Students are not permitted to have smart devices in school, other than their phone which must be kept in their locker at all times as per the Code of Behaviour.
  NB. Students are advised against bringing any valuable items to school (including phones) and the school does not accept responsibility for any damage, loss or theft of valuable items.

Internet Usage

- Students will not visit internet sites that contain obscene, illegal, hateful or otherwise objectionable and inappropriate materials.
- Students will use the internet for educational purposes only.
- Students will be familiar with copyright issues relating to online learning.
- Students will never disclose or publicise their own personal information or images online.
- Students will not disclose or publicise the personal information or images of others.
- Students will not comment, post images or respond to posts which could be regarded as disrespectful to other students, staff or other members of the school/local community.

  Internet content filtering is now centrally controlled by PDST. The content filtering option currently adopted by the school allows students to access a wide range of websites including educational, cultural and general interest categories while blocking potentially liable, objectionable or controversial content.

Email

- Students will use approved school email accounts under supervision by and permission from a teacher.
- Students will not send or receive any material that is illegal, obscene, defamatory or that is intended to upset, annoy or intimidate another person.
- Students will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.
- Students will never arrange a face-to-face meeting with someone they only know through emails or the internet.
- Students will note that sending and receiving email attachments is subject to permission from their teacher.
- Should students need to use their school email account from home they should follow the same rules and condition as in-school usage.

Internet Chat / Social Media

- Students do not have permission to access chat rooms and/or social media sites while on school premises.
- Students are informed of the risks associated with social media and chat apps along with the potential for cyber bullying via these modes of communication.

Use of Information and Communication Technology (ICT) Equipment

- Students must respect all computer/ICT equipment available in the school.
- The multimedia rooms and all other locations where computer equipment is made available must be kept clean and tidy at all times. Seating and desks in these areas must be used and maintained properly by all students with access to them.
- Any use of a piece of hardware for a purpose other than that for which it was provided by the school, will be considered misuse/abuse of that item.
- Removal of any piece of hardware/equipment from its designated location except under the express instruction of a staff member will be considered theft.
- Students must respect all software available in the school and ensure they do nothing to make that software unavailable to or harmful to other users.
- Students will not introduce software from outside the school environment via any medium except with the express permission of a staff member. It will be the responsibility of the relevant staff member to ensure any such software is virus free.

Sanctions

- Failure to observe any of the above clauses or deliberate breeches of the school's policy in relation to internet use and use of ICT equipment will lead to a student being refused permission to avail of the school's ICT equipment and facilities. Where use of ICT is deemed a vital part of a course being undertaken by that student a separate arrangement will be made between school management and parents/guardians.

- Furthermore, this policy will form part of the school's Code of Behaviour. Failure to comply with it will be treated as a disciplinary issue and depending on the nature of the offence, may incur any of the sanctions set out in the Code of Behaviour.

- The purpose of this Acceptable Use Policy is to ensure a safe, secure and efficient learning environment for all our students.

Guidance for Parents

- Internet usage and social media has become an integral part of life for many students.
- Many students have access to the internet through their own device.

- Please note that students are not permitted to use their own devices during school time.

- It is only on rare occasions that students will require access to the internet for set pieces of homework/study.

- It is important that students have guidelines and boundaries for their internet usage outside of school as well as those contained in this policy. We hope that you will find the following useful.

    - ❖ *Discuss the rules for using the internet and decide together when, how long, and what comprises appropriate use;*

    - ❖ *Get to know the sites your young person visits, and talk to them about what they are learning/viewing;*

    - ❖ *Insist that they seek your agreement before they give out personal identifying information in any electronic communication on the online, such as a picture, an address, a phone number, the school name, or financial information such as credit card or bank details. In this way you can help them to protect themselves from unwanted or unacceptable communications from strangers, from unplanned expenditure and from fraud;*

    - ❖ *Encourage your sons/daughters not to respond to any unwelcome, unpleasant or abusive messages, and to tell you if they receive any such messages or images. If the message comes via an internet service connection provided by the school, they should immediately inform the Principal.*

    - ❖ *Talk to them about the dangers of anonymous social media sites and the impact that these sites have on the mental wellbeing of young people.*

    - ❖ *See Appendix 1 for more tips for parents from www.webwise.ie*

Appendix 1

Social Media - **Tips for Parents** - www.webwise.ie

If your child using social media, here are a few conversation starters to help them make the most of the experience:

- Firstly, ask your child about what social networking services they use. Start on a positive footing by asking them to describe the things they like about it. Ask if you can see the profile. But don't be surprised if your child is reluctant to show you – children can see social networking as a parent-free zone where they communicate with friends.

- In order to open up the channels of communication with your child over their social networking use, don't be too critical of their online experience or habits to date. It's not always their fault if there is something inappropriate on their profile.

- Sometimes a teenager won't tell a parent about a bad experience they have had online because they fear that you might solve the problem by keeping them off their favourite social networking services. However, if they feel they can talk about their online habits with you, without judgement, or the threat of being disconnected it will lead to more honesty in the long run.

- Ask your child what privacy settings they have set up on their profiles. Encourage them if they are public, to amend the setting to private so that only friends can see what they post. But also let them know that even with the tightest privacy controls, content posted online can be easily copied and shared with audiences they can't control.

- It's a good idea too to talk about your child's friends list. "Friends" is the catch all term for any contacts on social networking sites. Sometimes, in their desire for popularity, teenagers become too relaxed about who they'll accept as 'friends'. Teenagers should review their list of online 'friends' regularly, so they are sharing their information only with people they trust.

- Be sure to put emphasis on the fact that they should NOT reply to any unwanted or unsolicited messages. Although it may seem obvious, often scam artists or predators use message which draw responses from young people. So it's good to make sure your child knows how important it is to ignore them

Managing Screen Time - **Tips for Parents** - www.webwise.ie

- Agree on a clear set of rules with your child on screen time in the home. Talk to your young person about when you think it is appropriate and inappropriate to use screens. Agree times when screens are allowed and not allowed in the home. For example dinner time, homework time and bedtime.

- Do as you say. Modelling behaviour is THE most powerful way you can influence your child's behaviour.

- Restrict the use of computers/devices in the bedroom. Depending on the age of your child you may want to set a curfew or ban devices from the bedroom completely.

- Buy an alarm clock for your child's bedroom and charge their phones in your room at night time. This can be a helpful way of giving them a break from the internet.

- Pick one evening a week where you do a family activity together, whether it's movie night, games night. Doing activities together as a family will help implement screen time guidelines and offer fun alternatives.

- Join in, why not set some time aside to play your child's favourite computer game and discover the online world together.

- Try not to rely on screens too much to keep the kids amused. It can be easy to encourage kids to pick up the tablet or play a game on the computer to keep them occupied. This only confuses rules on screen time, try and stick to the agreed rules with your child and remember to set a good example.

- Don't have screens always on in the background. Turn off TVs and Computers when not in use, these can be distracting for kids if they are trying to participate in another activity.

- Chat with your child about what they do online and encourage them to use their screen time for learning and education.

Webcam Blackmail – **Advice for Parents** - www.webwise.ie

Young people are using video and webcam chat to hang out with friends and meet new people. There are risks, such as webcam blackmail that can arise from the inappropriate use of these services. As with all other issues, proactive parenting can have a big impact on reducing the risks. We have put together some talking points to help you talk about the issue with your child. There is a video available at https://www.webwise.ie/trending/webcam-blackmail-advice-for-parents/ on sextortion from the BBC may be a good starting point to show your child an example of what webcam blackmail is and will illustrate how convincing pre-recorded footage can be.

- Remind your child that sometimes people aren't who they say they are. It may look and feel as if you talking to a real person when in fact it is a video recording. This can be very convincing and children/young people have more of a tendency to believe what they see.

- Talk to your child about using friends only setting on their social media sites. In many cases of webcam blackmail/sextortion, criminals initially make contact with victims via popular social networking sites. Children should always be wary of accepting friends or speaking online with someone they do not know.

- Ask your child if they think it is possible to pretend to be someone else in a live video chat.

- Ask your child what they could do to make sure the person they are chatting with is who they appear to be

- Young people or children are often aware of the dangers of sharing images or video, however, they may not realise how easy it is for the other person to record the video chat session and share it online. For this reason, children often feel that they can be freer in video chat as it feels like there is no record that the content they broadcast disappears into the ether. However, it is very easy to record without them knowing. The 'Granny Rule' is often helpful when discussing sharing private pictures/video online. Ask your child to consider before sharing anything online how they would feel if their Granny saw pictures/footage of them.

- Make an agreement with your child on suitable privacy settings for social networks. It's a good idea to keep accounts set to 'friends only'. This helps avoid strangers from making contact.