ICT Acceptable Use Policy 2020- 2021

Killina Presentation Secondary School Killina,
Rahan, Tullamore, Co. Offaly.

Contents

Purpose

Killina Presentation Secondary 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.

All assistive technologies used by students.

All connections made through the school online learning platform Google Workspace for Education.

Introduction

This Acceptable Use Policy outlines the guidelines and behaviours that our students are expected to follow when using school technologies or when using personally-owned devices on the Killina Presentation Secondary School campus or at any activity organised by the school.

Internet use and access is considered a school resource and privilege. Therefore, if the school AUP is not adhered to, this privilege may be withdrawn, and appropriate sanctions will be imposed – as outlined in the AUP.

- Students are expected to follow the same rules for good behaviour and respectful conduct online as offline. These rules are found in Killina Presentation Secondary School's existing Code of Behaviour.
- Misuse of school resources may result in disciplinary action
- We make a reasonable effort to ensure students' safety and security online, but will not be held accountable for any harm or damages that result from misuse of school technologies
- Students are expected to alert his/her teacher immediately of any concerns for safety or security.

It is envisaged that AUP will be reviewed regularly but it is understood that this AUP has been agreed by the parent for the school-life of their child unless the policy is altered i.e. it will not be re-signed each year. Before signing, the AUP should be read carefully to ensure that the conditions of use are accepted and understood.

4 Technologies Covered

Killina Presentation Secondary School may provide students with access to a range of technologies. As new technologies emerge, Killina Presentation Secondary School may provide access to them also. The policies outlined in this document are intended to cover all the technologies used in the school, now and in the future.

4.1 Killina Presentation Secondary School's : ICT Network

Killina Presentation Secondary School computer network is intended for educational purposes

- All activity over the network may be monitored and retained
- Access to online content via the network is restricted in accordance with our policies and the Department of Education and Skills and the NCTE.
- The web filter is a safety precaution, and no attempt should be made to circumvent it when using the internet.
- If a site is blocked and a student believes it shouldn't be, the student can ask his/her teacher to submit the site for review.

4.2 Killina Presentation Secondary School's: Email and Online Collaboration Tools

Killina Presentation Secondary School provides students with email accounts for school-related communication. Email accounts should be used with care. Email usage may be monitored and archived.
Students are expected to communicate with the same appropriate, safe, mindful and courteous conduct online as offline.

4.3 Killina Presentation Secondary School: IT Devices

Killina Presentation Secondary School may provide students with mobile computers, digital recorders, cameras, camcorders or other devices to promote learning both inside and outside of the school. Students should abide by the same expected use policies, when using school devices off the school network, as on the school network.

Students are expected to treat these devices with respect. They should report any loss, damage, or malfunction to their teacher staff immediately. Students may be financially accountable for any damage resulting from negligence or misuse.

4.4 Killina Presentation Secondary School: Security

Students and staff alike are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programmes and not opening files or programmes of unknown or untrusted origin.

5 Roles & Responsibilities

- 5.1 School Management
-
- The Board of Management will approve the policy and ensure its development, monitoring and evaluation.
- The Principal and Deputy Principal will be responsible for the dissemination of the policy and the application of sanctions.
- The Principal and Deputy Principal(s) will be responsible for the provision of training for students and teachers on the topic of internet safety and the effective and responsible use of ICT.
- The Principal and Deputy Principal(s) will be responsible for the scheduling of workshops and guest speakers on the topic of internet safety for parents and students.
- The school community will provide support for students who have been victims of online bullying by implementing our Anti-Bullying Policy.

5.2 Teachers

- Teachers will always monitor sessions during which electronic devices are being used.
- Teachers will outline to their classes, when appropriate, uses of Social Media, as part of the SPHE programme and as part of Well Being programmes..
- Class teachers will advise students on safe internet use as appropriate during lessons.
- Teachers will report incidents of online bullying and be mindful of the obligations under Child Protection Guidelines.

5.3 Parents

- Parents will be expected to read, understand and sign a contract on the Expected Use of ICT and Social Media in Killina Presentation Secondary School.
- Parents will help their children to read and understand said contract.
- Parents are expected to actively engage with their children, and to educate themselves, on Social Media issues.
- Parents will advise their children on the safe use of the internet, and the appropriate use of Social Media
- As the School A.U.P has been signed by all pupils and parents alike, let them understand that, as with any case of bullying, Killina Presentation Secondary

School takes these cyberbullying threats very seriously and will take appropriate measures to prevent them.

- Appendix A: Advice for Parents on Internet Safety

6 Electronic Communication

- Communication between pupils and staff, by whatever method, should take place within clear, professional boundaries. This includes the wider use of technology such as mobile phones, text messaging, emails, digital cameras, videos, webcams, websites and blogs.

- Teachers can be contacted via the school phone number. Staff should not give their personal mobile numbers or personal email addresses to pupils. For school business, except in exceptional circumstances, staff should not use their personal mobile numbers or personal email addresses. Whilst we recognise that as a tight knit community, many staff and parents have a social relationship as well as a professional relationship, in order that lines not be blurred, we ask that when possible and practical, staff should conduct school business through school channels. We recommend that parents only contact staff through official school channels where school business is concerned. We expect both parents and staff to understand and respect the difference between personal and professional business.

- Staff should not request, nor respond to, any personal contact made by a pupil to them on a social media site and should inform school management immediately of same.

- Members of the school community need to ensure that when they are communicating about others, even outside school, that they give due regard to the potential consequences of such comments. Making comments or allegations on social networking sites about others connected with the school could result in formal action being taken against them. This includes the uploading of photographs that might bring a person, persons or the school into disrepute.

7. Cyberbullying

This refers to bullying carried out using the internet, mobile phone or other technological devices. Cyberbullying can take many forms:

- Texts
- Sending nasty, mean or threatening messages, emails, photos or video clips
- Silent phone calls
- Putting up nasty posts or pictures online on 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 them.
- Misuse of any other medium/technological device.

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 will 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 impacts on school life).

8 Social Media Use

8.1 Guidelines for staff on the use of Social Media Sites

The use of Social Media sites by staff is governed by the recently published Code of Professional Conduct from the Teaching Council. Teachers shall:

- Communicate effectively with pupils, colleagues, parents, school management and others in a manner that is professional, collaborative and supportive, and based on trust and respect.
- Ensure that any communication with pupils, colleagues, parents and school management is appropriate, including communication via electronic media, such as email, texting and social networking sites.
- Ensure that they do not access, download or otherwise have in their possession while engaged in school activities, inappropriate or illegal materials/images in electronic or other format.
- 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.

8.2 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.

9. Student Responsibilities

9.1 Personal Safety

- If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the immediate attention of:
    - a teacher if you are at school
    - a parent / guardian if you are at home
- Students should never share personal information about themselves or others, including phone numbers, addresses, PPS numbers and birth-dates over the Internet without adult permission
- Students should never agree to meet someone they meet online in real life without parental permission.

9.2 Netiquette

Netiquette may be defined as appropriate social behaviour over computer networks and in the online environment. To this end:

- Students should always use the Internet, network resources, and online sites in a courteous and respectful manner
- Students should also recognize that among the valuable content online is unverified, incorrect, or inappropriate content. Students should use trusted sources when conducting research via the Internet
- Students should not to post anything online that they wouldn't want parents, teachers, or future colleges or employers to see. Once something is online, it is out there forever and can sometimes be shared and spread in ways you never intended.

More detailed examples of expected use and unacceptable use are given in Appendices B and C.

9.3 Network Security

- Use common sense if you think a website does not look right. Inform your teacher or parent.
- If you believe a computer or mobile device you are using might be infected with a virus, please alert your teacher or parent.
- Do not attempt to remove the virus yourself or download any programmes to help remove the virus. Students should not download or attempt to download or run .exe programmes over the school network or onto school resources.
- You will usually have permission to download other file types, such as images or videos. For the security of our network, download such files only from reputable sites, and only for educational purposes.
- No hacking attempt should be made on the school network or domain.

9.4 Plagiarism

- Students should not copy content, including words or images, from the Internet or use content as your own without citing the original creator. This is called plagiarism.
- Students should not take credit for things they didn't create themselves or misrepresent themselves as an author or creator of something found online.
- Research conducted via the Internet should be appropriately cited, giving credit to the original author
- The school may check for plagiarism using online tools as are available for such purposes
- The school will encourage students who create original content to claim ownership of it using a Creative Commons licence.

9.5 Cyberbullying

- Don't be mean. Don't send emails or post comments or photos with the intent of scaring, hurting, or intimidating someone else.
- Engaging in any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges
- Harassing, flaming, denigrating, impersonating, outing, tricking, excluding and cyber-stalking are all examples of cyber-bullying.
- In some cases, cyber-bullying is a crime
- Remember that your activities are monitored and retained
- Such bullying will not be tolerated in Killina Presentation Secondary School.

10. Sanctions for Infringements of this Policy

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
- Implementation of sanctions as per the Code of Behaviour.
- Suspension from school and school- related activities
- Exclusion
- Reporting to the Gardaí, and subsequent 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.

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.

11 Working From Home

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. .

• 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.

• 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 save or cache the username / password on your personal device.
- Once you are back at school, conduct a search of all devices to ensure that your personal data is deleted and work related files are moved to the school cloud. (Drive on G Suite.)

Protocol for Live Classes

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 can 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.

• In the event of a student becoming disruptive in class the following escalation policy will be followed:

o The student will be instructed to behave.

o If the disruption persists the student will be removed from the online class. At this point the school's code of behaviour will then apply.

Appendix A: Advice for Parents on Internet Safety

- Be informed about your child's internet use so that going online is a positive experience for you and your child.
- Try to keep the lines of communication open with your child and foster openness that they feel they can come to you if an issue does come up.
- Treat your child going on the internet as you would them going on a trip to O'Connell Street on their own. Find out who they're hanging out with, what they're doing and imagine what the potential hazards are. Online, there is no guard outside the GPO, there are no helpful bystanders and unlike being approached by a stranger in O'Connell Street, there is no way of telling exactly who you're communicating with online.
- Discover the internet together, parental guidance on internet use places your child at an advantage and develops a positive attitude to internet exploration and makes it easier to share positive and negative experiences in the future
- Agree with your child rules for internet use in your home
- Agree on how to treat personal information - encourage your child never to give out personal name, address, username, password or location. Check your child's privacy settings and location settings.
- Many games have an online messaging element, ensure that you understand this and know who your child is interacting with.
- Discuss how to behave towards others when gaming, chatting, e-mailing and messaging. Encourage your child to be responsible for what they post online. Encourage them to own up if they are wrong. We are all learning about responsible internet use.
- Teach your child that all comments posted online can be traced to the IP address of their internet device-nothing is anonymous. If you pay the bill or provide the Wi-Fi, you're legally responsible for anything that happens online on that account. This is crucially important if other children are using your Wi-Fi
- Social media sites like Viber, Whatsapp, Snapchat, Facebook, Twitter, Kik, Oovoo etc. have an age rating of 13.
- Be aware that some social media sites are set up by unknown groups with different agendas. Your child may be at risk.
- Teach your child that Skype, Facetime and other webcam sites are for family and closely selected friends.
- Teach your child that posting a photograph online has ramifications, the image is there forever, can be passed on and can be exploited. Once the digital image is online, it is out of your hands. A photograph doesn't disappear forever after a number of seconds.
- Be careful about allowing your child free access to Youtube. They can gain access to a lot of inappropriate material. Dangerous challenges that are put up on Youtube encourage children to copy them.
- Be aware that if your child has posted images or videos of themselves on Youtube or elsewhere online. The Internet has a vast audience. Making a video and posting it on Youtube may be dangerous.
- Agree on what types of sites and activities are OK in your family. Be involved with the sites your child is engaged with, know how they work. Not engaging is not an option.

- Talk about the risks associated with meeting online 'friends' in person. Teach your child not to meet anyone, stranger or otherwise, without your permission.
- Teach your child about evaluating information and being critically aware of information found online.
- Report online material you may consider illegal to the appropriate authorities.
- Encourage respect for others and help stamp out cyber-bullying. Encourage your children to REPORT, BLOCK and TELL if they are being cyberbullied. Do not retaliate. Record everything- keep all text messages, keep a note of calls, screen shot images and messages.
- Teach your child to protect their phone with a password and encourage them to share the password with you. Starting this practice at a young age can help you gain access to your child's virtual world. Download a child-friendly search engine to filter age appropriate material for your child.
- Let your children show you what they like to do online, be aware of how they are using the internet.
- Do not let your child have their internet device in their bedroom. Do not let them use it late at night or unsupervised. Internet use should be in a common space to encourage openness and to enable monitoring. There should be restrictions on time usage.
- Use filtering software designed to help parents limit the web-sites children can access.

N.B (If you are completely unsure when it comes to the Internet, gaming, social media and general technology, be open, seek help from the school or friends - We are all learning!)

Internet safety sites and links:
www.webwise.ie
www.internetsafetyday.ie
www.digizen.org
www.esafety.ie
www.thinkuknow.co.uk

Appendix B: Examples of Expected Use

I will:

- Use school technologies for school-related activities and research.
- Follow the same guidelines for respectful, responsible behaviour online that I am expected to follow offline.
- Treat school resources carefully, and alert teachers if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a teacher if I see threatening/bullying, inappropriate, or harmful content (images, messages, postings) online.
- Use school technologies at appropriate times, in approved places, for educational pursuits only.
- Student profile picture should be appropriate to a school settting. A head shot is suggested.
- Cite sources when using online sites and resources for research; ensure there is no copyright infringement.
- Recognise that use of school technologies is a privilege and treat it as such.
- Be cautious to protect the safety of myself and others.
- Help to protect the security of school resources.

This is not intended to be an exhaustive list. Students should use their own good judgment when using school technologies.

Appendix C: Examples of Unacceptable Use

I will not:

- Use school technologies in a way that could be personally or physically harmful to myself or others.
- Search inappropriate images or content.
- Engage in cyber-bullying, harassment, or disrespectful conduct toward others.
- Try to find ways to circumvent the school's safety measures and filtering tools.
- Use school technologies to send spam or chain mail.
- Plagiarise content (copy, use as their own, without citing the original creator) I find online.
- Post personally-identifying information, about myself or others.
- Agree to meet someone I meet online in real life.
- Use language online that would be unacceptable in the classroom.
- Use school technologies for illegal activities or to pursue information on such activities.
- Attempt to access sites, servers, accounts, or content that isn't intended for my use.
  This is not intended to be an exhaustive list. Students should use their own good judgment when using school technologies.

Appendix D: Internet Safety Contract

I will

- I will only use ICT in school for school purposes. I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will follow the same guidelines for respectful, responsible behaviour online that I am expected to follow offline.
- I will alert a teacher if I see threatening/bullying, inappropriate or harmful content (images, messages or posts) online.
- I will be cautious to protect the safety of myself of others.
- I will help to protect the security of the school's resources.
- I will only open/delete my own files. I will not access other people's files.
- I will ask the permission of the teacher before using the internet.
- I will only send e-mail messages, using a class or school e-mail address with my teacher's approval. The messages I send will be polite and responsible.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will treat my username and password like my toothbrush – I will not share it nor will I use any other person's username or password.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

I will not

- I will not engage in making negative comments about others, forwarding comments or 'liking' negative comments or images of others in the school community.
- I will not engage in cyber-bullying, harassment, or disrespectful conduct towards others in school or out of school.
- I will not agree to meet in real life someone I meet online.
- I will not use language online that would be unacceptable in the classroom.
- I will not deliberately look for, save or send anything that could be inappropriate or offensive. If I accidentally find anything like this, I will close the screen and tell a teacher/parent immediately as this will protect other children and myself.
- I will not give my full name, my home address or telephone number nor those of any others online.

I understand

- I understand the school can check my computer files and the Internet sites I visit, and that my parent/guardian will be contacted if a member of staff is concerned about my safety.
- I understand that the school also has the right to take action against me, in line with other school policies if I am involved in incidents of inappropriate behaviour when I am out of school and where they involve my membership of the school community (for example Cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with the Rules for Responsible Internet Use Agreement. I will be subject to disciplinary action.

Parental Acceptance and Consent

I have read and discussed this Expected Use Policy with my child and accept it.

Parent / Guardian Printed Name	Student Printed Name
Parent / Guardian Signature	Student Signature

Date

Photograph use at school events

Killina Presentation Secondary School uses its website, Facebook page and Twitter account to promote and support various activities that take place in the school. We have done this successfully for many years without incident.

If you do not want your child's photo on the school's website, we will make every effort that it does not appear.

This can be challenging, and mistakes may be made. If we inadvertently place a picture on the site, we will take it down as soon as possible after it has been brought to our attention.

I do not wish my child's photo to appear on the school website

Parent / Guardian Printed Name	Student Printed Name
Parent / Guardian Signature	Student Signature

Date