Kishoge Community College
Internet and ICT Acceptable Use Policy (AUP)

Adopted by the Board of Management 13th May 2015

A copy of the ICT AUP will be available on the school website. A printed copy will be furnished to parents on request.

Introduction

Kishoge Community College recognises that access to Information and Communication Technology (ICT) gives our students enhanced opportunities to develop skills that will equip them for 21st century life. For this reason, Kishoge Community College provides access to ICT for student use. 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 inside Kishoge Community College campus or at Kishoge Community College organised events.

Technologies Covered

Kishoge Community College may provide students with internet access, access to 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, Kishoge Community College may provide access to them also. The policies outlined in this document are intended to cover all online and offline technologies used in the school, not just those specifically mentioned. As new technologies are incorporated into Kishoge Community College, this policy may be updated accordingly. This policy should be read in conjunction with Kishoge Community College's *iPad Acceptable Use Policy.*

Kishoge Community College ICT Network

Kishoge Community College computer network is intended for educational purposes. Access to ICT is considered a school resource and a privilege. Therefore, if the school AUP is not adhered to, this privilege will be withdrawn and appropriate sanctions, as outlined in this AUP, will be imposed.

- 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 policies of the Department of Education and Skills through its agency, the National Centre for Technology in Education.
- Students are expected to respect that the web filter is a safety precaution and should not try to circumvent it when browsing the web. 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.
- Proxy servers are strictly forbidden. Any attempt to circumvent the internet filtering system is a serious breach of this AUP.

- Students should not engage in any activity online which is in breach of local, national or international law.
- Students should not engage in any activity which may bring Kishoge Community College, its staff or student body into disrepute.
- Students are expected to follow the same rules for good behaviour and respectful conduct online as offline – these rules are found in Kishoge Community College's *Code of Positive 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.
- A student is expected to alert his/her teacher immediately of any concerns for safety or security.

Kishoge Community College email and online collaboration
Kishoge Community College provides students with email accounts for the purpose of school-related communication. Availability and use is restricted in line with school policies. Email accounts should be used with care. Email usage may be monitored and archived. Kishoge Community College recognises that online collaboration is essential to education and may provide students with access to a variety of online tools that allow communication, sharing, and messaging among students. Students are expected to communicate with the same appropriate, safe, mindful and courteous conduct online as offline.

Kishoge Community College Security
Students are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes, but is not limited to, not opening or distributing infected files or programmes and not opening files or programmes of unknown or untrusted origin. Students are expected to use common sense: if student thinks a website does not look right he/she must inform a teacher. If a student believes a computer or mobile device might be infected with a virus he/she must alert a teacher (in school) or a parent/guardian (at home). Student should not attempt to remove the virus him/herself 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. Students may be permitted to download other file types, such as images or videos. For the security of the school network, such files should only be downloaded from reputable sites and only for educational purposes.

Netiquette
Netiquette may be defined as 'appropriate social behaviour over computer networks and in particular in the online environment'. To this end:
- Students should always use the internet, network resources, and online sites in a courteous and respectful manner
- The internet should be used for educational purposes only.

- Students should also recognise that in addition to the valuable content online, there is often unverified, incorrect, or inappropriate content. Students should use trusted sources when conducting research via the internet.
- Students should not post anything online that they wouldn't want parents, teachers, or future colleges or employers to see.

Plagiarism
- Students should not plagiarise (copy or use as your own without citing the original creator)) content, including words or images, from the internet.
- 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.

Personal Safety
If you see a message, comment, image, or anything else online that makes you concerned for your personal safety or the safety of others, 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. Any breach of this will be seen as a serious breach of school rules and will carry with it appropriate sanctions.
- Students should never agree to meet someone they meet online in real life without parental permission.

Cyber-bullying
The Department of Education and Skills defines cyberbullying as; "placing a ***once-off*** offensive or hurtful public message, image or statement on a social network site or other public forum where that message, image or statement can be viewed and/or repeated by other people."

Harassing, 'flaming', denigrating, impersonating, outing, tricking, excluding and cyber-stalking are all examples of cyber-bullying.
- Such bullying will not be tolerated in Kishoge Community College. See Kishoge Community College's *Anti-bullying Policy.*
- Inappropriate actions on social media sites can also constitute bullying, e.g. "liking" degrading comments/photos on Facebook, Trolling etc.
- 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 disciplinary action and loss of ICT privileges.
- In some cases cyber-bullying is a crime and may be reported to the Garda.
- Students are advised that activities are monitored and retained.
- The school will support students, teachers and parents in dealing with cyber-bullying.

Violations of this Acceptable Use Policy

Violations of this policy in Kishoge Community College may have disciplinary repercussions including but not limited to:

- Suspension of network and computer privileges
- Notification to parents
- Detention
- Suspension from school and/or school-related activities
- Expulsion
- Legal action and/or prosecution
- Kishoge Community College reserves the right to report any illegal activities to the appropriate authorities, such as the Garda.

Queries related to ICT in Kishoge Community College may be directed to kishogeIT@gmail.com

Acceptance Form

Please read Kishoge Community College's *ICT Acceptable Use Policy* and indicate acceptance by signing below:

Student:

I agree to use ICT in a responsible way in full compliance with the *ICT Acceptable Use Policy.*

Name of Student: _____

Student's signature: _____

Parent/Guardian:

As the parent or legal guardian of the above student, I have read the *ICT Acceptable Use Policy* and grant permission for my son/daughter or the child in my care to access the internet. I understand that internet access is intended for educational purposes. I also understand that every reasonable precaution has been taken by the school to provide for online safety but the school cannot be held responsible if students access unsuitable websites.

I agree to support the school's AUP by appropriate monitoring of home internet use.

Parent's Name: _____

Parent's Signature: _____