HIGH CROSS
COLLEGE

Acceptable Use Policy

Introduction

High Cross College provides access to various computer resources, including the school network and the internet. These resources are available to facilitate the learning process in a supportive school environment and to provide quality learning outcomes for our students. The school encourages students to become familiar with the use of information technology in the achievement of learning outcomes and personal learning goals.

The responsible use of internet and digital technologies, both online and offline and access is considered an integral part of teaching and learning.

It is envisaged that school and parent representatives will revise the A.U.P. annually. Before signing, the A.U.P. should be read carefully to ensure that the conditions of use are accepted and understood.
The aim of this policy is to ensure that pupils will benefit from learning opportunities by the school's internet resources in a safe and effective manner. Internet use and access is considered a school resource and privilege. Therefore, if the school policy is not adhered to this privilege may be withdrawn and the appropriate sanctions will be imposed.

Definitions

- AUP: Acceptable Use Policy
- ICT: Information Communication Technologies (devices)
- GSuite (is the suite of resources made available by Google: Gmail, Chrome,Google Classroom etc.)
- Hardware: Physical parts of a computer e.g. monitor, mouse and keyboard
- Operating System: Software that manages the resources of a computer and allows the application software to run.
- Applications Software: Programs that run on a computer, e.g. word, spreadsheets.
- Server: A powerful computer that controls access to all other computers.

- Internet: Worldwide connected network of computers used to share information.
- WWW: World Wide Web can be considered a virtual library of information.
- Email: Electronic Mail.
- Wi-Fi: Wireless fidelity. Data is exchanged between devices wirelessly.

Rationale for this policy

This policy is intended to give guidance and direction for the acceptable use of I.C.T. as appropriate for all members of the school community (i.e. students, staff, parents and approved visitors/speakers etc.) who have access to, and who are users, of our I.C.T., GSuite network and the school's Local Area Network (L.A.N.).

When using GSuite, Zoom, any ICT, and Compass in High Cross College, all members of the school community are expected:

- To take good care of all school I.C.T. equipment and use it responsibly in accordance with school policy.
- To treat other users with respect at all times.
- To respect the right to privacy of all members of the school community.
- To respect copyright and acknowledge creators when using online content and resources.
- Not to engage in behaviours or misuse ICT resources in a manner that would bring the school into disrepute.

Scope of Policy

Students are expected to adhere to this policy throughout their time with us as students of High Cross College. The school also reserves the right to report any illegal or inappropriate activities to the relevant statutory authorities i.e. Gardaí, TUSLA. Office of the Data Commissioner etc.

This policy must be read in conjunction with all other school policies including;

- GDPR Policy
- Child Protection Policy
- Code of Positive Behaviour
- Anti-Bullying Policy
- Mobile Phone Policy

Acceptable Use Policy for Students

Every time a student enters a username and password in order to use the School's Computers, GSuite Network, email, Google Classroom, Google Meets, Zoom and Compass they agree to the following rules:

- Students will report any damages found prior to use. The school reserves the right to seek compensation for damages

to computers.

- Students will act responsibly when using computers. All gaming and social networking sites are NOT permitted unless instructed to use by a teacher.
- The student agrees to have their computer sessions monitored via classroom control software.
- Any violation of the above will lead to restorative action by the school Management.

- Uploading and downloading of non-approved software will not be permitted.
- Virus protection software will be used and updated on school devices on a regular basis.

The school employs a number of strategies in order to maximise learning opportunities and reduce risks associated with I.C.T. These strategies are as follows:

General

- Students must use their own username and password assigned to them by the school when using GSuite and our I.C.T.equipment.
- All students will be issued with a GSuite package. This will provide access to Google (GSuite) applications such as email (@highcrosscollege.ie), cloud storage, communication and collaboration platform (Googlemeets, Google Classroom and Zoom) and video streaming service. Students are encouraged to save their work to their GSuite or google classroom account rather than on the school network or on personal devices.
- Access to the GSuite package will be withdrawn within 12 months of a student leaving the school.
- The school reserves the right to monitor students' activity on GSuite to ensure that it is being used appropriately and for educational purposes only. Students should seek permission from their teacher before sharing any content using their GSuite account with another member of the school community. Students should also be mindful of copyright infringements and plagiarism when sharing material via GSuite. Please note activity of users on GSuite is automatically recorded by the system. Reports of user activity are available to school management.

- Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.
- Students must not create websites, pages, groups or other social media accounts, which reference the school, to express personal opinions without the prior approval of school management. Students must not create, transmit, display, publish or forward any material that is likely to harass, cause offence to any person or bring the school into disrepute. High Cross College reserves the right to protect the reputation of the school.
- Uploading and downloading of non-approved software will not be permitted.
- Virus protection software will be used and updated on school devices on a regular basis.

Content Filtering

High Cross College has chosen to implement the following level on content filtering on the Schools Broadband Network:

Level 4 This level allows access to millions of websites including games and YouTube but blocks access to websites belonging to the personal websites category and websites such as Facebook belonging to the Social Networking category.

Students taking steps to by-pass the content filter by using proxy sites or other means may be subject to disciplinary action, including written warnings, withdrawal of access privileges, detention and, in extreme cases, suspension or expulsion.

World Wide Web/ Internet usage

-
- Internet sessions in the school will be supervised by a teacher
- Students will not intentionally visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Filtering software and/or equivalent systems will be used in the school in order to minimise the risk of exposure to inappropriate material.
- Students will be encouraged to report accidental accessing of inappropriate materials in accordance with school procedures via your teacher or Year Head
- Students will use the Internet in the school 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 materials or images not relevant to their studies, is in direct

breach of the school's Acceptable Use Policy.

- Students will not engage in online activities such as uploading or downloading large files that result in heavy network traffic which impairs the service for other internet users.
- Students and staff 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.
- Students will not download or view any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.
- Students will never disclose or publicise personal information or passwords.
- Students will be aware that any usage of the internet and school's digital platform, including distributing or receiving information, school-related or personal, will be monitored.

Email

- Students will only use their approved school Gmail (@highcrosscollege.ie) accounts for school correspondence. All staff and students will be issued with a school email account.
- The use of personal email addresses is not allowed for school based work.
- Students must only use their school email for school related activities and for registering on school based activities only.
- Students should not under any circumstances share their email account login details with other pupils.
- Students should not use school email accounts to register for online services such as social networking services, apps, and games.
- Students should be cognisant that Gmail can be traced back to place,date, and time of sending.
- Prior to sending an email, students must ensure that they are satisfied with the content and should double check the address of the intended recipient. Once the "send" key is pressed, the e-mail cannot be stopped or retrieved. Deleting mail from your system does not make it untraceable.
- Students will not instigate or forward "junk mail" to users either within or outside the school
- Students will not forward email messages or screenshots of emails or "reply all" without the permission of the originator.
- Students will not send or receive any material that is illegal, obscene, and 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, 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.

- Students should immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Students should avoid opening emails that appear suspicious. If in doubt, pupils should ask their teacher before opening emails from unknown senders.
- All emails and opinions expressed in emails are the responsibility of the author and do not reflect the opinion of the school.

Internet Chat

- In the school, students will only have access to chat rooms, discussion forums, messaging or other electronic communication that have been approved by their teacher.
- Discussion forums and other electronic communication forums will only be used for educational purposes and will always be supervised.
- Face-to-face meetings with someone organised via Internet chat is forbidden.

School Social Media/Website

The internet provides a range of social media tools that allow us to interact and keep in touch. While recognising the benefits of these media tools for new opportunities for communication, this policy sets out the principles that members of your school community are expected to follow when using social media.

The principles set out in this policy are designed to help ensure that social media is used responsibly so that the confidentiality of pupils and other staff and the reputation of the school is protected.

This policy applies to personal websites such as social networking sites (for example Instagram and TikTok), blogs, microblogs such as Twitter, chatrooms, forums, podcasts, open access online encyclopaedias such as Wikipedia, social bookmarking sites such as del.icio.us and content sharing sites such as flickr and YouTube. The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media.

The following statements apply to the use of messaging, blogging and video streaming services in High Cross College :

- Use of instant messaging services and apps including Snapchat, WhatsApp, Viber, etc. is allowed at certain times in High Cross College .
- Use of video streaming sites such as YouTube is allowed at certain times in High Cross College.

All members of the school community must not use social media, messaging services and the internet in any way to harass, impersonate, insult, abuse or defame others.

Staff and students must not discuss personal information about pupils, staff and other members of the High Cross College community on social media.

Staff and students must not use school email addresses for setting up personal social media accounts or to communicate through such media.

Staff and students must not engage in activities involving social media which might bring High Cross College into disrepute.

Students will be provided with guidance on etiquette regarding social media.

Teachers can read further information about the use of Social Media and Electronic Communication here:

https://www.teachingcouncil.ie/en/news-events/latest-news/2021/guidance-for-registered-teachers-about-the-use-of-social-media-and-electronic-communication.html

- The school website and social media accounts operate under the authority of the B.O.M. and is managed by members of the school staff on behalf of the school.

- The school Twitter,Instagram and Facebook accounts post regular updates of school news, notices, and activities. High Cross College also retweets relevant information to other twitter users as appropriate. Permission is obtained from parents/ guardians at enrolment to allow photographs of their son/daughter to be published on the school website.
- The school YouTube and Zoom channels host videos of school activities and performances.
- Students without website permission may be asked by their teacher to step out of photographs/videos etc that are intended for the school website. If the school inadvertently displays an image without the appropriate consent it will be removed immediately on the school being made aware of the error.
- Students may on occasion be given the opportunity to publish schoolwork on the school website.
- Personal student information including home address and contact details will be omitted from school web pages.
- The school will ensure that image files are appropriately named.

Recording of Images & Video

Care should be taken when taking photographic or video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Students must not share images, videos, or other content online which could be deemed harmful to another member of the school community either in school or out of school. Recording of online classes without the consent of all those present is strictly prohibited.
- Classes recorded by teachers and made available to students are to remain the property of the teacher and high Cross College. They must not be viewed, downloaded, shared, published, or distributed without the permission of the teacher and school management.
- Written permission from parents or guardians will be obtained upon enrollment photographs of students are published on the school website.
- The school permits the recording of images and videos of students and school activities once permission has been sought and granted. Students may only take photos or videos on school grounds or when participating in school activities using the school digital cameras as directed by a teacher.
- Students must not take, use, share, publish or distribute images of any member of the school community except with the permission of the teacher and member of the school community.
- Sharing explicit images and in particular explicit images of students and/or minors is an unacceptable and absolutely prohibited behaviour, with serious consequences and sanctions for those involved. Sharing explicit images of other students automatically incurs suspension as a sanction.

Use of Digital Learning Platforms (including video conferencing)

High Cross College digital learning platform is owned and managed by the school. This platform should enable two-way communication.

Students must only use their school email for accessing the school digital learning platform.

All school-related media and data should be stored on the school's platform.

The use of digital platforms should be used in line with considerations set out in the school's data protection plan (GDPR).

Each user of the platform will be provided with their own unique login credentials.

Passwords for digital platforms and accounts should not be shared.

Personal email addresses should not be used when creating accounts on school digital platforms.

Prior acceptance from parents should be sought for student usage of the schools' digital learning platform.

- Our school utilises teleconferencing during periods of school closure. Distance learning is a way of learning remotely without being in regular face-to-face contact with a teacher in the classroom. There are many benefits to teaching and learning in this way, and students and teachers have the tools and expertise to use teleconferencing to sustain learning.

Our school provides a video conferencing option within Google Classroom for our students and staff. It is expected that students and staff will use the platform in a professional and ethical manner for the purpose of teaching, learning and assessment.

The use of teleconferencing requires students to observe the following rules in order to ensure that both staff and students benefit from this way of teaching and learning. Students must not:

- Post, stream or transmit any content, including live video, that violates this Policy in such a way that is offensive to students / staff.
- Do anything illegal, facilitate any illegal activity, or promote violence.
- Do anything that threatens, exploits, or otherwise harms others.
- Engage in any activity that is harmful, obscene, or indecent. This includes offensive gestures, displays of nudity, violence, pornography, sexually explicit material, or criminal activity.
- Engage in any activity that is fraudulent, false, or misleading.
- Engage in any activity that is defamatory, harassing, threatening or abusive.
- Store or transmit any data or material that is fraudulent, unlawful, harassing,

libellous, threatening, obscene, indecent, or otherwise inappropriate.

- Send unauthorised messages or irrelevant material.
- Misrepresent a user's identity or affiliation with any entity or organisation or impersonate any

  other people.
- Harvest,collect or gather user data without consent. This includes screen recording

  or taking screenshots during online classes.
- Violate or infringe any intellectual property or proprietary rights of others, including copyrights.
- Violate the privacy of others or distribute confidential or personal information of others.

Cyberbullying

This type of bullying is increasingly common and is continuously evolving. It is bullying carried out through the use of information and communication technologies such as text, social media, e-mail, messaging, apps, gaming sites, chat-rooms and other online technologies. Being the target of inappropriate or hurtful messages is the most common form of online bullying. As cyberbullying uses technology to perpetrate bullying behaviour and does not require face to face contact, cyber-bullying can occur at any time (day or night). Many forms of bullying can be facilitated through cyber-bullying. For example, a target may be sent homophobic text messages or pictures may be posted with negative comments about a person's sexuality, appearance etc.

Access to technology means that cyberbullying can happen around the clock and the students home may not even be a safe haven from such bullying. Students are increasingly communicating in ways that are often unknown to adults and free from supervision. The nature of these technologies means digital content can be shared and seen by a very wide audience almost instantly and is almost impossible to delete permanently. While cyberbullying often takes place at home and at night, the impact can also be felt in school.

In accordance with the Anti-Bullying Procedures for Schools, High Cross College considers that even 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 will be regarded as bullying behaviour.

When using the internet students, parents and staff are expected to treat others with respect at all times.

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.

Measures are taken by High Cross College to ensure that staff and students are aware that bullying is defined as unwanted negative behaviour, verbal, psychological or physical, conducted by an individual or group against another person (or persons) and which is repeated over time. This definition includes cyberbullying even when it happens outside the school or at night. In addition the Department of Education Anti-Bullying Procedures, 2013 defines cyberbullying as "placing a once-off offensive or hurtful public message, image or statement on a social network site or another public forum where that message, image or statement can be viewed and/or repeated by other people will be regarded as bullying behaviour".

The prevention of cyberbullying is an integral part of the anti-bullying policy of our school.

Cyberbullying, like all bullying, can have terrible effects on those experiencing it. It can lower your self-esteem and you may feel alone, sad, angry and scared. If you are being bullied it is not your fault and there is nothing wrong with you. Don't be afraid to tell someone you are being bullied.

What to do:

- If you are being cyberbullied, keep a record (including time and date) this may help you (or the school) to find out who is sending the messages.
- Tell some – talk to someone you trust, a parent, a friend, school counsellor, chaplain or teacher.

- Contact your mobile phone or internet service provider and report what is happening – they can help you block messages or calls from certain senders.
- Don't reply to bullying messages – it may get worse if you do

Responsible Internet Use

These rules will help us to be fair to others and keep everyone safe.

1. I will ask permission before using the Internet.
2. I will not look at or delete other people's files.
3. I will not bring software or external hard drives such as USB sticks into school without permission.
4. I will only email people I know, or my teacher has approved.
5. The messages I send will be polite and sensible.
6. I will not give my home address or phone number, or arrange to meet someone.
7. I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
8. I will not use Internet chat.
9. If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
10. I understand that the school may check my computer files and the Internet sites I visit.
11. I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

School Websites

Students will be given the opportunity to publish projects, artwork or school work on the internet in accordance with clear policies and approval processes regarding the content that can be loaded to the school's website.

Students will continue to own the copyright on any work published.

The website will be regularly checked to ensure that there is no content that compromises the safety, privacy, or reputation of students or staff.

Webpages allowing comments or user-generated content will be pre-moderated and checked frequently to ensure that they do not contain any inappropriate or offensive content.

High Cross College will use only digital photographs, audio or video clips of focusing on group activities. Content focusing on individual students will only be published on the school website with parental permission.

The publication of student work will be coordinated by a teacher.

Personal student information including home address and contact details will not be published on High Cross College web pages.

The school will ensure that the image files are appropriately named and will not use students' names in image file names or ALT tags if published online.

Bring Your Own Device/Personal Devices

Students using their own technology in school should follow the rules set out in this agreement, in the same way as if they were using school equipment.

The following statements apply to the use of internet-enabled devices such as mobile phones, tablets and smartwatches, in High Cross College:

- Students are only allowed to use personal internet-enabled devices during lessons with expressed permission from teaching staff.
- Students are allowed to use personal internet-enabled devices during social time, as per the agreed times during the school day, namely break and lunch time.
- Some students may be granted permission to use a personally owned mobile device within the school for educational purposes only. Use of a personally owned mobile device will be supervised and will only be permitted during class time. The school will decide on the type of allowed device allowed.
- Students must take responsibility for appropriate use of their personal device at all times. The school is not responsible in any way for personal devices or for its use.
- Students/parents/guardians are responsible for their devices, including any breakages, costs of repair, or replacement.
- The school reserves the right to inspect or monitor student mobile devices during school hours.
- Violations of any school policies or rules involving a student device may result in a student not being allowed to continue using the device during school hours and/or disciplinary action, for a period to be determined by the school.
- During school hours students are allowed to use their device for learning related activities only.
- Students must comply with teachers' requests regarding use of devices during school hours.
- Mobile devices must be charged prior to bringing them to school in order so as to be usable during school hours. Student use of charging devices in the school is not permitted.
- Students may not use the devices to record, transmit or post photos or video of other teachers or students. No images or video recorded at school can be transmitted or posted at any time without the supervising teacher's permission.
- Each user is responsible for her/his own device and should use it responsibly and appropriately. The school takes no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices.
- High Cross College is not responsible for any possible device charges to your account that might be incurred during approved school-related use.

Inappropriate Activities

- Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation.
- Misuse and fraud legislation.
- Racist material.
- Pornography.
- Promotion of any kind of discrimination.
- Promotion of racial or religious hatred.
- Harmful content or threatening behaviour, including promotion of physical violence or mental harm.
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school.
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions.
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords.)
- Creating or propagating computer viruses or other harmful files.
- Online gambling.
- Child sexual abuse material.
- Any other activity considered questionable .

Sanctions for the misuse of ICT and Internet by students

The misuse or unlawful use of the Internet or ICT equipment during school /class time by students will result in disciplinary action as outlined in the school's Code of Behaviour, Anti Bullying Policy, and Mobile Phone Policy. Sanctions may include withdrawal of access and privileges to ICT and other school related privileges and, in extremely serious cases, suspension or expulsion.
GSuite access may be withdrawn for a specified time.

The school also reserves the right to report any illegal or inappropriate activities to the relevant statutory authorities i.e. Gardaí, TUSLA. Office of the Data Commissioner etc.

ICT and Legislation - the following legislation is relevant to Internet Safety.

The school will provide information on the following legislation relating to use of the Internet which teachers, students and parents should familiarise themselves with:

Data Protection Act 2018- this act gives effect to the General Data Protection Regulation (GDPR) May 2018 in the Irish context.

Data Protection Act 1998 - this act was passed in order to deal with privacy issues arising from the increasing amount of information kept on a computer about individuals.

Data Protection (Amendment) Act 2003 - this amendment extends the data protection rules to manually held records and also makes improvements to the public's right to access data.

Child Trafficking and Pornography Act 1998 - this act legislates against anyone who knowingly produces, prints, publishes, distributes, exports, imports, shows, possesses or sells child pornography.

Interception Act 1993 – this act stipulates that telecommunication messages can be intercepted for the purpose of an investigation of a serious offence. Authorisations are subject to certain conditions.

Video Recordings Act 1989 - this act prohibits the distribution of videos which contain obscene or indecent material which may lead to the depravation or corruption of the viewer.

Copyright and Related Rights Act 2000 – this act governs copyright in Ireland.

Children First Act 2015

Harassment, Harmful Communications and Related Offenses Act 2020 (Coco's Law.)

Criminal Damage Act 1991

Support Structures

The school will inform students and parents of key support structures and organisations that deal with illegal material or harmful use of the Internet.

Sanctions

Misuse of the Internet and digital technologies should be referred to in the school's Code of Behaviour and Anti-Bullying Policy and related sanctions regarding misuse as appropriate should be outlined therein. The school also reserves the right to report any illegal activities to the appropriate authorities, including An Garda Siochana.

Student and Parent/Guardian Acceptance of Acceptable Use ICT Policy

I agree to follow the school's Acceptable Use Policy on the use of the internet and digital technologies. I will use the internet and digital technologies in a responsible way and obey all the procedures outlined in the policy.

Student's Signature: _____

Parent/Guardian Signature : _____

Date: _____

As the parent or legal guardian of the above student, I have read the Acceptable Use Policy and 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.

In relation to the school website, I accept that, if the school considers it appropriate, my child's school work may be chosen for inclusion on the website. I understand and accept the terms of the Acceptable Use Policy relating to publishing students' work on the school website.

Signature: _____ Date: _____

Address: _____

_____

_____

_____

Please review the attached school Internet Acceptable Use Policy, and sign and return this permission form to the Principal.

School Name: Name of Student:_____

Class/Year:_____

Student:_____