

***New Cross College***

***Acceptable Use Policy***

This policy covers use of digital technologies in school, that is, email, internet, intranet and network resources, learning platform, software, equipment and systems and has been drawn up to protect everyone. The provisions of this policy also apply to access to the internet and email via remote devices such as smart phones and laptops.

***1. PURPOSE:***

New Cross College owns and operates a variety of computing systems, which are provided for the use of New Cross College students and staff in support of the programs of the school and are to be used for education, research, academic development, and public service only. All users\* of these systems are responsible for seeing that these computing facilities are used in an effective, efficient, ethical, and lawful manner. This document establishes rules and prohibitions that define acceptable use of these systems. Unacceptable use is prohibited, and is grounds for loss of computing privileges, as well as discipline or legal sanctions. \*User definition: A user is defined as an individual who uses a digital device.

***2. AUDIENCE AND AGREEMENT***

All users of New Cross College computing systems must read, understand, and comply with the policies outlined in this document, as well as any additional guidelines established by the Information Technology Department. Such guidelines will be reviewed by the I.C.T Co-ordinator.

***3. RIGHTS***

By using any of these systems, users agree that they will comply with these policies These computer systems, facilities, and accounts are owned and operated by New Cross College. New Cross College reserves all rights, including termination of service without notice, to the computing resources that it owns and operates. These procedures shall not be construed as a waiver of any rights of the school, nor shall they conflict with applicable acts of law.

***4. PRIVILEGES***

Access and privileges on New Cross College computing systems are assigned and managed by the ICT Co-ordinator. Eligible individuals may become authorized users of a system and be granted appropriate access and privileges by following the approval steps prescribed for that system by the ICT Co-ordinator. The ICT Co-ordinator must approve all access to the School’s computer resources, including the issuing of accounts and related passwords. Users may not, under any circumstances, transfer or confer these privileges to other individuals. Others shall not use any account assigned to an individual without express permission from the ICT Co-ordinator. The authorised user is responsible for the proper use of the system, including any password protection.

***5. RESPONSIBILITIES***

Users are responsible for maintaining the following:

a) An environment in which access to all School computing resources are shared equitably between users. The ICT Co-ordinator sets minimum guidelines within which users must conduct their activities.

b) An environment conducive to learning:

* A user who brings food or drink into the computer rooms will be asked to leave and privileges may be removed.
* Disruptive behaviour will not be tolerated in any form. If any arises, the user responsible will be denied access to the system and will be given alternative written work to complete at that time.
* A user who harasses, or makes defamatory remarks, shall bear full responsibility for his or her actions. Further, by using these systems, users agree that individuals who transmit such remarks, to or from the school, shall bear sole responsibility for their actions.

c) Users agree that New Cross College's role in managing these systems is only as an information carrier, and that they will never consider transmission through these systems as an endorsement of said transmission by New Cross College. Some of the NCC computing systems provide access to outside networks, both public and private, which furnish electronic mail, information services, bulletin boards, conferences, etc. Users are advised that they may encounter material that may be considered offensive or objectionable in nature or content. Users are further advised that New Cross College does not assume responsibility for the contents of any of these outside networks. The user agrees to comply with the acceptable use guidelines for whichever outside networks or services they may access through New Cross College systems. Further, the user agrees to follow proper etiquette on outside networks.

d) The user agrees never to attempt to transmit, or cause to be transmitted, any message in which the origination is deliberately misleading (except for those outside services which may conceal identities as part of the service). The user agrees that, in the unlikely event that someone does transmit, or cause to be transmitted, a message that is inconsistent with an environment conducive to learning or with a misleading origination, the person who performed the transmission will be solely accountable for the message, not New Cross College, which is acting solely as the information carrier.

e) An environment free of illegal or malicious acts: The user agrees never to use a system to perform an illegal or malicious act. Any attempt to increase the level of access to which they are authorised, or any attempt to deprive other authorized users of resources or access to any New Cross College computer system shall be regarded as malicious, and may be treated as an illegal act.

f) The user agrees to be bound by the terms and conditions laid down in the Data Protection Act of 1988 and the Freedom of Information Act of 1997 and to inform themselves of their rights as citizens and their responsibilities under said acts. Other legal / sector specific requirements need to be satisfied under the list of applicable Irish Laws as referenced in this document. All users agree to abide by the terms and conditions of these applicable Irish Laws.

g) A secure environment:

* When not in use the doors to the computer rooms must be kept locked.
* All computers in all rooms must be logged off when not in use.
* No user is permitted to use removable storage media that have originated outside of New Cross College. Storage solutions will be issued by the School, if needed.
* Any user who finds a possible security lapse, or technical difficulty, on any system is obliged to report it to the ICT Co-ordinator.
* Knowledge of passwords or of loopholes in computer security systems shall not be used to damage computing resources, obtain extra resources, take resources from another user, gain unauthorised access to resources or otherwise make use of computing resources for which proper authorization has not been given.
* Users are responsible for backup of their own data. The ICT Co-ordinator may from time to time schedule an overhaul and clean-up of the network. File owners will be notified of this necessary maintenance, in advance, if such notice is practical.
* All users must become familiar with logging off the system and must do so at the end of every session. If so asked by their teacher, users must ensure that all systems are shut down, through the proper means, when they are finished using them.

***6.ACCOUNTS***

Accounts will be issued and revoked solely by the ICT Co-ordinator. Others must not use an account assigned to an individual without express permission from the ICT Co-ordinator. The individual is responsible for the proper use of the account, including proper password protection. The user is responsible for all work carried out through and transmitted to and from the account issued and for maintenance of files and folders created within said account.

***7.CONFIDENTIALITY***

Programs and files are confidential unless they have been made available, with written permission, to other authorized individuals. The ICT Co-ordinator reserves the right to access all information stored on computers other than those used by senior management. File owners will be notified of file access and/or maintenance, in advance, if such notice is practical. When performing maintenance, every effort is made to insure the privacy of a user's files. However, if policy violations are discovered, they will be reported immediately.

***8. SYSTEM USAGE***

Users must be aware that all their computer activity is tracked and logged for reference purposes. These individual user logs may be accessed at any time by the ICT Co-ordinator. If policy violations are discovered they will be reported immediately. Electronic communications facilities (such as E-MAIL) are for school related activities only. Fraudulent, harassing or obscene messages and/or materials are not to be sent or stored. The computer facilities may be used during out of class times by any student who has been deemed competent in computer usage by a member of the ICT coordinating committee. Staff may use either of the Computer Rooms with their class group during class time provided the appropriate class periods are recorded via the booking procedures in force at that time. This rule applies to the booking of the laptop trollies. These should be booked in the staff room on the ICT timetable which goes up weekly. Block booking is available during CBA periods. ICT classes take precedence over all other sessions.

***9. SYSTEM PERFORMANCE***

No one should deliberately attempt to degrade the performance of a computer system or to deprive authorized personnel of resources or access to any school computer system.

***10. UNAUTHORIZED ACCESS***

Loopholes in computer security systems or knowledge of a special password should not be used to damage computer systems, obtain extra resources, take resources from another user, gain access to systems or use systems for which proper authorization has not been given.

***11. COPYRIGHT***

Computer software protected by copyright is not to be copied from, into, or by using New Cross College computing facilities, except as permitted by law or by the contract with the owner of the copyright. This means that such computer and microcomputer software may only be copied in order to make back-up copies, if permitted by the copyright owner. The number of copies and distribution of copies may not be done in such a way that the number of simultaneous users in a department exceeds the number of original copies purchased by that department.

***12. VIRUS PROTECTION***

Computer viruses are items of software that attach themselves to other legitimate items of software or data, without the consent of the computer user, and are programmed to proliferate themselves onto other computers, often to cause disruption or damage. It is essential that all users play a part in protecting the network from the presence of viruses. It is the policy of the school to run up to date virus protection software on all computers that are attached to the network. This software will automatically report the presence of most known viruses. Any user who receives an on-screen warning from this software (these are very clear and explicit) should stop all use of the computer immediately and report the occurrence to the ICT Co-ordinator or the ICT Technician. Removable storage media are not allowed to be used in school unless the device has been virus scanned before being connected to any computer on our school network. These must be re-scanned again each time they are used in computers outside the network. Please give reasonable notice to system administrators if scanning is needed.

***13. VIOLATIONS***

An individual's computer use privileges may be suspended immediately upon the discovery of a possible violation of these policies. Such suspected violations will be confidentially reported to the ICT Co-ordinator. The Principal may nominate the ICT Co-ordinator to conduct an examination of computing systems at any time and without prior notice to assure compliance with internal policies, assist with internal investigations, and assist with the management and protection of the school’s information resource systems. Violations of these policies will be dealt with in the same manner as violations of other school policies and may result in disciplinary action. In such a review, the full range of disciplinary sanctions is available including the loss of computer use privileges, dismissal from the school, Garda involvement and legal action. Violations of some of the above policies may constitute a criminal offence.

***DML AT NEW CROSS COLLEGE:***

* New Cross College offers timetabled classes for Information Technology in 1st-3rd Year, Transition Year and Leaving Cert Applied.
* Teachers are encouraged to take their classes to the computer room where the Internet can be used as a virtual library of information.
* In general classrooms, staff and students have access to a laptop, data projector, screens, speakers and in some classis’s interactive whiteboards.
* There are two trolleys of laptops available. One for upstairs classrooms and the other for downstairs classrooms.
* A device contract is signed by these teachers
* Students have access to Virtual Learning Environments (VLE) in certain subject areas.
* An approved VLE is the preferred means of communication between teacher and student. It is much less prone to the abuse prevalent in other social media and provides the necessary framework for teacher-student and student-student interaction in a controlled environment. At the moment Office 365 is the VLE being used in New Cross College.
* Students and teachers work can be saved either to a single server and as a result files are accessible from any computer that is networked or to the students/teachers own One Drive in Office 365

***Related school policies:***

* Code of Behaviour
* Anti-Bullying
* Child Protection Guidelines
* Data Protection

***Legislation***

Students, parents/guardians and teachers should familiarize themselves with legislation relating to the use of the internet.

* Data Protection (Amendment) Act 2003
* Child Trafficking and Pornography Act 1998
* Interception Act 1993
* Video Recordings Act 1989
* The Data Protection Act 1988

***Cyberbullying/ Misuse of the Internet or Social Media***

* Bullying is 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 following types of bullying behaviour are included in the definition of bullying:

deliberate exclusion, malicious gossip and other forms of relational bullying, cyber-bullying, Identity-based bullying such as homophobic bullying, racist bullying, bullying based on a person’s membership of the Traveller community and bullying of those with disabilities or additional educational needs.

* Cyberbullying is bullying carried out through the use of information and communication technologies such as text, social networking sites, email, instant messaging (IM), apps, gaming sites, chat-rooms and other online technologies. Being the target of inappropriate or hurtful messages/videos is the most common form of online bullying. Cyber-bullying uses technology to perpetrate bullying behaviour and does not require face-to-face contact.
* Isolated or once-off incidents of intentional negative behaviour, including a once-off offensive or hurtful text message or other private messaging, do not fall within the definition of bullying and should be dealt with, as appropriate, in accordance with the school’s code of behaviour.
* In the context of this policy, 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 will be regarded as bullying behaviour.
* Negative behaviour that does not meet this definition of bullying will be dealt with in accordance with the school’s code of behaviour.
* Reports of cyberbullying will be recorded on a Bullying/Cyberbullying Incident Form and will be dealt with under the Anti-Bullying Policy and the Code of Behaviour.

***School’s strategies for safe use of the internet:***

New Cross College employs a number of strategies in order to maximise learning

opportunities and reduce risks associated with the Internet. These strategies are as follows:

1. AUP Forms: All users will be presented with an appropriate acceptable use policy document in line with their role in the school.

In August each year, all Staff must sign to acknowledge that they have and accept this AUP document. Student AUP forms are in the student journal. Once these forms have been signed in the journal, the user will have access to the computing systems in operation throughout the school.

2. Present “Cyberbullying, Advice to students: how to stay safe on the internet” to all student users. This can be done in Wellbeing class/ DML.

3. Teach students about the appropriate use of social media.

4. Enforce school rules on mobile phones and internet use

5. Make this policy available to parents/guardians and all users on the school website

6. Advise parents/guardians to discuss safe internet usage with their sons/daughters

7. Provide in service training for staff on teaching practice.

8. Ensure Internet sessions are always supervised by a teacher.

9. Use filtering software and/or equivalent systems in order to minimise the risk of exposure to inappropriate material.

10. The school regularly monitors students’ Internet usage. All computer rooms including the language lab have monitoring system software.

11. Uploading and downloading of non-approved software is not permitted.

12. Virus protection software is used and updated on a regular basis.

13. The use of personal USB keys in school is not permitted.

14. Students sign in at a computer and sign out when class is finished. This allows the school to know who has worked at any particular computer at any time.

***E-mail:***

16. Students will use approved email accounts under supervision and only with permission from a staff teaching member and only these accounts must be used when communicating approved work to or from the school.

17. Staff will use approved email accounts when communicating professionally with other partners in education or significant bodies regarding school or educational business.

18. Non-school related business will be conducted using a non-school email account.

***Discussion Forums***

19. Students will only have access to discussion forums or other electronic communication forums that have been approved by the school.

20. Discussion forums and other electronic communication forums will only be used for educational purposes and will always be supervised.

21. Usernames will be used to avoid disclosure of identity.

22. Face-to-face meetings with someone organised via Internet chat are forbidden.

***School Website***

23. We are privileged to have a portal on the World Wide Web that gives interested parties an insight into the life of the school. This exists at www.newcross.ie. It is envisaged that our students will contribute to the site and they will be given the opportunity to publish projects, artwork or school work on the World Wide Web.

24. The publication of student work will be co-ordinated by a staff member.

25. Students’ work will appear in an educational context on Web pages with a copyright notice prohibiting the copying of such work without express written permission.

26. Digital photographs, audio or video clips of students will only be published on the school website with parental/guardian permission. This is located in journal where it should be signed by parents.

27. Personal student information including home address and contact details will be omitted from school web pages.

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

***Strategies for guiding teacher practice:***

Teachers in this school:

* Adhere to the Teaching Council’s Code of Professional conduct
* Adhere to the school’s AUP document
* Deliver “Cyberbullying: Advice to students”
* Share resources for learning more about cyberbullying and safe internet use

***User Responsibilities***

All users will:

* not visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials
* be familiar with copyright issues relating to online learning.
* never disclose or publicise personal information.
* 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.
* be aware that use of Internet social network sites such as Facebook, Twitter, YouTube, etc. both inside and outside the school, must not bring the good name of New Cross College, or any teacher or student of the school, into disrepute. As stated in the school’s Code of Behaviour. Their ‘out of school’ conduct must not in any way undermine the reputation of the school.
* be advised of the permanent and public nature of posts made on social media and the potential consequences for future career prospects which inappropriate material may represent.

***Student responsibilities:***

* Students should read and consider the definition of cyberbullying as set out in this document.
* Students must sign the AUP form in the Student Journal and agree to comply with this policy.
* Students will use the Internet for educational purposes only.
* Students 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 use approved email accounts for school business only.
* Students will not send or request to receive any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.
* Students will not use removable storage media without permission from a staff member who has had the device scanned for possible viruses.
* Students should report any concerns about internet usage to staff
* Students should report inappropriate material on the web on school computers.
* Students will observe good “netiquette” (i.e., etiquette on the Internet) at all times and will not undertake any actions that may bring the school into disrepute.
* 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.

***Sanctions***

* The aim of this Acceptable Use Policy is to ensure that all users will benefit from learning opportunities offered 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 AUP is not adhered to, this privilege may be withdrawn and appropriate sanctions may be imposed as per the Code of Behaviour.
* The school also reserves the right to report any illegal activities to the appropriate authorities, to involve the Gardai and other legal bodies should the need arise in the case of a serious breach of this AUP.
* Circulating, publishing or distributing (including on the internet) material associated with school activities including but not limited to material in relation to staff and students where such circulation undermines, humiliates or causes damage to another person is considered a serious breach of school discipline and may result in disciplinary action.

***Internet safety resources:***

* http://www.internetsafety.ie/ The Office for Internet Safety has been established by the Irish Government to take a lead responsibility for internet safety in Ireland, particularly as it relates to children.
* http://www.webwise.ie An excellent resource that covers much of what schools, teachers and parents/guardians need to know in order to deal effectively with cyberbullying. This site is managed by the NCTE.
* <http://www.spunout.ie/health/Healthy-mind/Bullying/Cyber-Bullying>

SpunOut is an independent, youth led national charity working to empower young people between the ages of 16 and 25 to provide an interactive online community for young people to consume health and lifestyle information and find out about health and advice services available to them in their area, online or over the phone.

* http://ie.reachout.com/inform-yourself/bullying-and-personal-safety/cyber-bullying/.
* ReachOut.com is an Irish service dedicated to taking the mystery out of mental health by providing quality assured mental health information and inspiring real-life stories by young people to help other young people get through tough times.ReachOut.com is run by the Inspire Ireland Foundation which is a not for profit, non-government registered charity.
* www.watchyourspace.ie Clear succinct advice on managing children’s profiles on social networking sites.
* EU Kids Online Hugely informative on the way young people use modern communications technology and contains a specific report on how Irish young people use these technologies and the risks and safety for young people in Ireland using the Internet.
* Homophobic bullying is a major cause of unhappiness among young people. BeLonG To, an organisation for LGBTQIA+ young people, aged between 14 and 23 is an excellent resource in addressing this type of bullying. Each year BeLonG To organise a Stand Up Awareness Week aimed at creating a positive understanding of LGBTQIA+ issues.

Signed: 

Chairperson of the Board of Management

22/2/23