



ICT ACCEPTABLE USE FOR STUDENTS

This policy adheres to and should be applied with due consideration to the College's commitment to the Framework for Ethical Leadership in Education.

This policy has been reviewed in line with the Sustainable Development Goals.

Mission Statement

Our mission inspired by the Christian tradition is to be a community based on faith, hope and love; developing each individual intellectually, emotionally and spiritually to achieve their full potential.

To achieve this we will:

- Provide a welcoming, supportive community where everyone is valued.
- Provide a high quality, meaningful education which encourages the development of the whole person, inspired by the Notre Dame tradition.
- Promote a caring environment, rooted in the virtues of service, kindness, gratitude and respect.
- Work together for the benefit of each person as well as the wider community.
- Recognise, celebrate and treasure, without exception, the unique gifts and dignity of each person, ensuring equality and fairness for all, as found in the teaching and example of Our Lord Jesus Christ.

Author	IT Network and Services Manager
Date Reviewed	January 2025
Approved by SLT	January 2025
Approved by Audit Committee	February 2025
Review interval	1 year
Policy Last reviewed	January 2024
Policy to be reviewed by or before	January 2026

The use of the latest technology is actively encouraged at Notre Dame Catholic Sixth Form College. With this comes a responsibility to protect students, staff and the College from abuse of its systems.

All students, therefore, **must** adhere to the policy set out below. This policy covers all computers, laptops and electronic devices within the College Network, irrespective of who owns the device. Failure to comply with the terms of this Policy may be dealt with as a Disciplinary matter under the Student Code of Conduct.

Students are expected to behave responsibly on the College computer network and with the IT equipment, as they would in classrooms and in other areas of the College.

The following points should be noted:

- Personal use should be limited, for example, you must not use the Internet to conduct transactions on-line, however you can use it to research topics of personal interest.
- You must not use College computers or services for outside business interests; however it would be acceptable to prepare letters, use a spreadsheet or prepare other documents for personal use.
- Whilst the College recognises that you will not always be able to stop a personal e-mail from being received, external personal e-mail should not be encouraged, for example, by giving out your College email address to personal contacts or signing up for e-mail alerts. Personal external e-mails should only be sent occasionally and out of core hours. *See Section 7 below.*
- Personal usage should be within the bounds of the law and decency. You should ensure appropriate courtesy and respect to others. You should not, for example, use your College e-mail address to express your personal views on issues which may be seen to be related to the College since such use could extend liability for those views to the College as a whole. Disparaging remarks about others should not be made.
- For the avoidance of doubt, no sexually explicit or racist material, indecent images or any material likely to cause offence or embarrassment to others should be created, downloaded or accessed.
- You should only visit chat rooms directly related to work purposes, *see Section 4 below on inappropriate Behaviour.*
- Any damage to College IT equipment, accidental or intentional may be subject to financial compensation.

1.0 E-safety and Social media

Please see the relevant Social and Media Policy.

2.0 Information Security Management

The following statements about computer security are applicable to the use of any College computer system and also need to be adhered to when using remote access software to use College computers through the internet.

2.1 I will keep my password secure (secret) and will never give it to anybody else to use.

2.2 I understand that my student logon gives me access to systems and information that other students are not entitled to access and I will not under any circumstances allow anyone else access to a computer under my logon credentials.

- 2.3 I will not leave an unattended computer logged in and will always log off when I finish using a College computer.
- 2.4 If I think someone else has obtained my logon details, I will report it to IT support staff as soon as possible and ensure that my password is changed.
- 2.5 I will use computers with care and leave IT equipment as I found it. I will not tamper with computer systems or devices (e.g. printers and projectors) and their cabling.
- 2.6 If I notice that IT equipment or software is damaged or not working correctly, I will report it by emailing itsupport@notredamecoll.ac.uk straight away.
- 2.7 I will not try to bypass security features or systems in place on the network or try to access resources or user account files that I do not have permission for (hacking).
- 2.8 If I find that I do have access to an area that I know I should not have access to I will inform IT Support immediately.
- 2.9 I will never knowingly bring a computer virus, spyware or malware into College.
- 2.10 If I think a College computer or a removable storage device that I am using contains a virus, spyware or other malware I will inform IT Support.
- 2.11 I will not open an attachment or download a file unless I know and trust the person who has sent it.
- 2.12 I will not attempt to go beyond my authorised access. This includes attempting to log on as another person, sending email whilst pretending to be another person or accessing another person's files. I am only permitted to log on as myself.
- 2.13 I will not attempt to connect to another user's laptop or device while at College. I am not permitted to establish my own computer network.
- 2.14 I will never attempt to install software on College computers or mobile devices myself (unless I have the permission of IT support staff) and will request a software change by emailing itsupport@notredamecoll.ac.uk.
- 2.15 I will not knowingly install spyware or any sort of hacking software or device.
- 2.16 I will try to prevent people from watching me enter passwords or viewing sensitive information.
- 2.17 If I lose or misplace any College owned portable ICT equipment, I will inform IT Support immediately.
- 2.18 I understand that access to many sites on the internet is blocked. I will not attempt to bypass these blocks in any way. If a site is blocked which I believe is needed for my course, I will request with my Teacher/Tutor that it be made available by emailing IT Support.

- 2.19 I understand that 3rd party VPNs and proxy anonymisers must not be used to access college resources, unless explicitly authorised by IT Support. For example, use of a VPN app to access email from home or when connected to the College Wi-Fi.
- 2.20 I understand that Multi Factor Authentication (MFA) will be required to access my Office 365 account externally.
- 2.21 The College recognises the benefits that can be achieved by allowing students to use their own electronic devices for College work, whether that is at home, on campus or while travelling. Such devices include laptops, smart phones and tablets, and the practice is commonly known as 'bring your own device' or BYOD.
- 2.22 I must invoke all the relevant available security features on personal (BYOD) devices, including firewalls, ensuring that antimalware is performing daily scans and scanning web pages.
- 2.23 On personal (BYOD) devices, I must take all reasonable steps to:
- Prevent theft and loss of data
 - Keep information confidential where appropriate
 - Maintain the integrity of data and information, including that on the college site.
 - Take responsibility for any software downloaded onto the device
 - Set up passwords, passcodes, passkeys or biometric equivalents. These must be of sufficient length and complexity for the particular type of device. They should be a minimum of 6 characters/numbers in length.
 - Ensure that no college information is left on any personal device indefinitely. Care must be taken if a device is disposed of/sold/transferred to a third party.
- 2.24 I must not install unsigned applications and not 'root' or 'jailbreak' my BYOD devices.
- 2.25 I understand that any personal (BYOD) devices connected to the College Wi-Fi must not run any peer-to-peer apps or software.
- 2.26 I understand that if my personal (BYOD) device compromises the security or performance of the College network, then it could be immediately blocked from accessing the BYOD network.

3.0 Inappropriate Behaviour

- 3.1 I will not store, download or distribute music, video or image files on my personal user space unless they are appropriately licensed media files (*e.g.* Creative Commons licensed files) that I need for College.
- 3.2 I will not use indecent, obscene, offensive or threatening language.
- 3.3 I will not engage in personal, prejudicial or discriminatory attacks.
- 3.4 I will not send or post defamatory or malicious information about a person or about College as this may breach the Malicious Communications Act 1988, Computer Misuse Act 1990.
- 3.5 I will not post or send private information about another person.

- 3.6 I understand that bullying, manipulation or exploitation of another person either by email, online or via texts will be treated with the highest severity.
- 3.7 I will not use the internet for gambling.
- 3.8 I will not access material that is profane or obscene, or that encourages illegal acts, violence or discrimination towards other people. If I mistakenly access such material I will inform my tutor or another member of staff immediately or I may be held responsible.
- 3.9 If I am planning any activity which might risk breaking the IT Acceptable Use Policy (*e.g.* research into gun laws for a legitimate project), I will inform a member of staff beforehand to gain permission.
- 3.10 I will not attempt to use proxy sites on the internet. I will not attempt to bypass any security systems that the College has put in place to access sites that have been blocked.
- 3.11 I will not take a photo or video of another student or member of staff without their permission.
- 3.12 I will not bring computer game files into College or store them on my personal user space and I will not play computer games in lessons without permission from my tutor.

4.0 Monitoring

It should be noted that the College does not currently monitor the content of e-mails as a matter of routine. However, it should also be noted that, where there is reason to believe that the law or College policy or procedures have been broken, the content of emails may come under scrutiny.

The activity on the system which may be audited for the purposes of compliance with this policy include:

- All Internet use is logged to display date, time, username, and target URL (the website visited)
- All attempts to access blocked sites
- All e-mail use will be logged to display date, time, username; and the address to which the message is being sent
- All remote access to the College resources will be logged to display the date, time and username of all users accessing the service.

If misuse is suspected, an investigation will take place and this may result in disciplinary action. All audits and logs will be retained in line with the College GDPR policy and guidelines.

- 4.1 I understand that all files and emails on the College computer system and cloud platforms are the property of the College. As such, system administrators and staff have the right to access them if requested.
- 4.2 I understand that all network access, web browsing and emails on the College system and laptops are logged and may be routinely monitored without my knowledge.

4.3 I understand that the College reserves the right to randomly search the internet for inappropriate material posted by users and to act upon it.

5.0 Printing

As an organisation we continually try to reduce the cost and negative environmental impact of printing.

5.1 I understand that the College provides access to shared multi-function devices as a main source of printing and I will use these devices to print to whenever possible.

5.2 I will not use College printing facilities to print materials which are not related to College work.

5.3 I will only print out work that I need as a paper copy – where possible I will use College systems such as Teams, OneDrive, email, Outlook groups and shared folders to share information electronically.

5.4 If I believe a printer is not working or out of toner I will inform reprographics or tell a member of staff.

5.5 I will not print on glossy paper, card or acetate on College printers, except in specialist subjects (Art/ Photography) where I have explicit permission from a teacher.

5.6 I will not tamper with any printing/ copying equipment.

5.7 I will always seek to apply the most economical use of resources when printing/copying.

5.8 I understand that the College provides a credit system for printing. This is to reduce costs and save unnecessary printing. I understand that if needed I can purchase additional credits for this.

6.0 Email

6.1 I understand that my @ndonline.ac.uk email is a College email account and as such will be used for College purposes only.

6.2 I will only use my approved, secure @ndonline.ac.uk e-mail system for any College communication.

6.3 I understand that my email account will be closed at the end of the calendar year when I leave College and that it is my responsibility to ensure that any important information is transferred to a new email account and that my contacts are updated and made aware of the change.

6.4 I will only open email attachments from trusted senders.

6.5 I will not assume that any email sent on the internet is secure.

6.6 I will not reply to spam emails as this will result in more spam. I will delete all spam emails.

7.0 Best practice

- 7.1 I will save work regularly using sensible file names.
- 7.2 I will organise my files in a sensible manner and tidy my user space regularly.
- 7.3 Wherever possible I will save work on my College OneDrive account. If work has to be saved to a different location for a legitimate reason, I understand that it is my responsibility to back this up to OneDrive.
- 7.4 I will regularly back up any work that is not saved on the College network or the OneDrive cloud storage.
- 7.5 I will observe health and safety guidelines when using computer equipment.
- 7.6 I will be considerate and polite to other users.
- 7.7 When I graduate College, I understand that my account will be disabled at the end of October and I will ensure that I save any files that I wish to keep. If I leave the College before I graduate, I understand that my account will be disabled immediately. I understand that my account will be deleted at the end of the academic after it has been initially disabled but may be temporarily re-enabled if my request is approved.
- 7.8 I will not connect music/video players to the College network, College computers or speakers without permission from my tutor.
- 7.9 I will only empty my recycle bin when I am certain I no longer need the files.
- 7.10 I will not eat while using computers and I will ensure that any drink I have is covered with a lid.
- 7.11 I am aware that portable device such as USB drives must be encrypted before they are connected to College systems.

8.0 Data Protection

All students will ensure that:

- 8.1 I will comply with the College GDPR Policy and guidelines.
- 8.2 I will not share data protected information (including College images) with third party organisations without seeking permission first.
- 8.3 I will only use remote access, my OneDrive storage, my College email account or an encrypted USB device to access the College Network from off-site.
- 8.4 I will not store files containing data protected information on a home computer or mobile device.
- 8.5 I understand that leaving a computer logged on and unattended may result in a breach of the GDPR/Data Protection Act and leave 'personal data' unprotected.

8.6 I am aware that portable device such as USB drives must be encrypted before they are connected to College systems.

9.0 Remote lessons

9.1 General rules and expectations: all students are expected to follow the general rules for acceptable behaviour when using ICT as in the ICT acceptable use Policy and the Classroom Code of Conduct.

9.2 Students should arrive on time for each session and remain engaged throughout the whole session.

9.3 Students must be dressed appropriately at all times.

9.4 Students must never send or accept invites to join Teams from anyone other than a teacher/tutor or member of staff from Notre Dame. Please note this could be a criminal offence under The Computer Misuse Act.

9.5 Students should ensure face to face communication is only between teachers and students. Any parent/carer to teacher communication should be in the usual manner.

9.6 Students should behave in a respectful, polite and courteous manner at all times. The use of any profanity and offensive comments - written, drawn, displayed or spoken - during a meeting is unacceptable and appropriate disciplinary action will be taken.

9.7 Students should not upload, share or forward material that could be considered offensive, inappropriate or illegal. If they do, appropriate disciplinary action will be taken.

9.8 Students should not share any personal information with anybody online.

9.9 You **MUST NOT** record each other's online interactions or take any screen shots. If the lesson is to be recorded, this will be done by the teacher.

9.10 If teachers, tutors or staff at Notre Dame use live 1-2-1 sessions with students, they will be recorded for safeguarding purposes.

10.0 Sanctions

10.1 All students must understand that failure to comply with any part of this policy may lead to disciplinary action.

10.2 If my actions cause damage to computer equipment, I will be charged for the cost of repairing items broken or damaged through carelessness or vandalism.

10.3 I may also be charged for the cost of correcting problems caused by hacking or tampering.

10.4 I understand that sanctions will vary depending on the severity of the offence, from a warning or withdrawal of internet use to sanctions under the Code of Conduct which may include: suspension or expulsion. Any breach of the law may lead to the involvement of the Police.