Notre Dame Catholic Sixth Form College

IT ACCEPTABLE USE
POLICY FOR STUDENTS

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:

• The purpose for 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 e-mail 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.*

1.0   Access

As a student at Notre Dame, I have access to the following IT facilities:

1.01   Computers throughout the College campus.

1.02   A secure username and password for logging into College computer systems.

1.03   An accredited, filtered Internet connection from any computer in College or Wi-Fi connected device.

1.04   My Documents personal user space on the College network of up to 2 Gigabytes:

1.05   Personal Microsoft OneDrive for Business user space with 1 Terabyte of storage through my email account.

1.06   A personal @ndCollege.ac.uk email account with 50 Gigabytes of email storage space.

1.07   Access to network printers and copiers. All students are given an allocation of printing funds, c£5, at the start of the College year and each page printed is charged out, dependant on colour etc. If necessary additional printing funds can be purchased at the Finance Office.

1.08   Access to resources such as scanners, digital cameras, laptops and video cameras (dependant on courses taken and department resources).

1.09   Access to the following licensed software for home computer use:

        i.   Microsoft Office 365 online
        ii.   Microsoft Office Professional on up to five devices
        iii.   ClickView Online

1.10   A personal Moodle account, providing both internal and remote access to online resources and virtual learning environment functionality, for the courses that you take.

1.11   A personal CEDAR account providing access to your data on attendance and attainment.

1.12   Access to shared resources such as the Work drive on the College network.

1.13   Access to the College NotreDame-StudentWiFi for internet access with your personal IT devices.

1.14   Access to the Open Access IT Area and the Library IT systems throughout the College day.

1.15   IT Support from the technicians helpdesk on the IT floor, through email to: itsupport@notredamecoll.ac.uk or through tweets to @ndCollegeits

2.0   E-safety

2.01   I will take all reasonable steps to ensure that I am aware of e-safety issues affecting young people, and I will use the e-safety resources on the College network to promote this.

2.02   I will only email individuals that I know or that my tutors have approved.

2.03   The messages I send, or information I upload, will always be polite and sensible.

2.04   When I use internet sites, I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family, my friends, other students or staff members unless my tutor has given permission.

2.05   I will never arrange to meet someone I have only ever previously met on the internet or by email or in a chat room unless my parent or guardian has given me permission and I take a responsible adult with me.

2.06   If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a member of staff.

2.07   If I access inappropriate material by accident (*e.g.* on a website) I will tell a member of staff.

2.08   I will not send anyone my credit card or bank account details without checking that it is a secure website with https at the start of the web address.

2.09   I will always be myself and will not pretend to be anyone or anything that I am not on the internet.

2.10   I will not use email or any communication technology to bully or harass others and I will report instances of online bullying to a member of staff.

2.11   I understand that if someone makes me an offer via email or the internet that seems too good to be true, it probably is.

2.12   If I am in doubt I will ask a member of staff.

3.0   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.

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

3.02   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.

3.03   I will not leave an unattended computer logged in and will always log off when I finish using a College computer.

3.04   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.

3.05   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.

3.06   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.

3.07   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).

3.08   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.

3.09   I will never knowingly bring a computer virus, spyware or malware into College.

3.10   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.

3.11   I will not open an attachment, or download a file unless I know and trust the person who has sent it.

3.12   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.

3.13   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.

3.14   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.

3.15   I will not knowingly install spyware or any sort of hacking software or device.

3.16   I will try to prevent people from watching me enter passwords or viewing sensitive information.

3.17   If I lose or misplace any College owned portable ICT equipment I will inform IT Support immediately.

3.18   I understand that access to many sites on the internet is blocked. I will not attempt in any way to bypass these blocks. If a site is blocked which I believe is needed for my coursework I will request with a member of staff that it be made available.

4.0   Inappropriate Behaviour

4.01   I will not post any material on any social media platform that may cause offence to anyone or bring the College into disrepute; see also Section 10 below.

4.02   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.

4.03   I will not use indecent, obscene, offensive or threatening language.

4.04   I will not engage in personal, prejudicial or discriminatory attacks.

4.05   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.

4.06   I will not post or send private information about another person.

4.07   I understand that bullying, manipulation or exploitation of another person either by email, online or via texts will be treated with the highest severity.

4.08   I will not use the internet for gambling.

4.09   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.

4.10   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.

4.11   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 in order to access sites that have been blocked.

4.12   I will not take a photo or video of another student or member of staff without their permission.

4.13   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.

5.0   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 network will be logged to display the date, time and user name 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.

5.01   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.

5.02   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.

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

6.0   Printing

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

6.01   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.

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

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

6.04   If I believe a printer is not working or out of toner I will inform reprographics, IT Support, or tell a member of staff.

6.05   I will not print on glossy paper, card or acetate on College printers.

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

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

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

7.0   Email

7.01   I understand that my @ndonline.ac.uk email is a College email account, linked to my College photograph, and as such will be used for College purposes.

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

7.03   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.

7.04   I will only open email attachments from trusted senders.

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

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

8.0   Best practice

8.01   I will save work regularly using sensible file names.

8.02   I will organise my files in a sensible manner and tidy my user space regularly.

8.03   Wherever possible I will save my work on the College network or on the OneDrive for Business cloud storage that I have access to.

8.04   I will regularly back up any work that is not saved on the College network or the OneDrive for Business cloud storage.

8.05   I will observe health and safety guidelines when using computer equipment.

8.06   I will be considerate and polite to other users.

8.07   When I leave College permanently, I understand that my account will be closed at the end of the calendar year and I will ensure that I save any files that I wish to keep.

8.08   I will not connect music/video players to the College network, College computers or speakers without permission from my tutor.

8.09   I will only empty my recycle bin when I am certain I no longer need the files.

8.10   I will not eat while using computers and I will ensure that any drink I have is covered with a lid.

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

9.0   Data Protection

All students will ensure that:

9.01   I will comply with the College GDPR Policy and guidelines.

9.02   I will not share data protected information (including College images) with third party organisations without seeking permission first.

9.03   I will only use remote access, my OneDrive for Business storage, my College email account or an encrypted USB device to access the College Network from off-site.

9.04   I will not store files containing data protected information on a home computer or mobile device.

9.05   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.

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

10.0 Social Networking

Principles

Students who identify themselves as part of Notre Dame Catholic Sixth Form College:

- Must not engage in activities on the Internet which might bring the College into disrepute.
- Must act in a transparent manner when altering online sources of information.
- Must not use the Internet in any way to attack or abuse students, teachers or others. This may be classed as cyber bullying and may be dealt with under the College Disciplinary Procedures.
- Must not post derogatory comments, or comments of an offensive nature, on the Internet.

All students will ensure that:

10.01 I will not load photos or videos of another person to websites or social networking sites without their permission.

10.02 I will never access a member of staff's private social networking profile or that of their friends and families.

10.03 I will never create a bogus social networking account or site that is associated with a member of staff, students or the College.

10.04 If I become aware of misuse of Social Networking accounts or sites that are associated with a member of staff, students or the College, I will inform IT Support or tell a member of staff.

11.0 Remote lessons

11.1 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.

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

11.3 Students must be dressed appropriately at all times.

11.4 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.

11.5 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.

11.6 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.

11.7 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.

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

11.9 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.

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

12.0   Sanctions

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

12.02 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.

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

12.04 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.

Reviewed June 2020

Next review due July 2021
(IT Network Manager)