NOTRE DAME COLLEGE

ACCEPTABLE USE - STUDENT INFORMATION, COMMUNICATIONS AND TECHNOLOGY SYSTEMS

POLICY AND PROCEDURE

INTRODUCTION

The *Student ICT Acceptable Use Policy and Procedure* consists of four sections. Please ensure you have read and understood each section prior to signing the '*Student and Parent/Guardian Notebook Agreement Acceptance'*.

SECTION A - The College Network

In this document Cloud refers to college managed Google Apps for Education (GAFE), Microsoft Office 365/One Drive (Office 365) or any other service provided by the college which is not hosted on services residing on the Notre Dame College premises.

The term "Network" refers to **all** computing equipment provided by the College and **all** software and services operating on that equipment. This includes, but is not limited to:

- Notebook and Desktop computers
- Publishing and browsing on the Internet (including Intranet and Extranet)
- Downloading or accessing files from the Internet or other electronic sources
- Email
- Electronic bulletins/notice boards
- Electronic discussion/news groups
- Weblogs ('blogs')
- File transfer
- File storage
- File sharing
- Video conferencing
- Streaming media
- Instant messaging
- Online discussion groups and "chat" facilities
- Subscriptions to list servers, mailing lists or other like services
- Copying, saving or distributing files
- Viewing material electronically
- Printing material

1. Access to the College Network

Access to the College's Network and use of ICT at the College is a privilege, not a right. No one is permitted to access the College's Network without:

- Reading and understanding this policy.
- Authorisation from the College via an individual and confidential password.

2. Acceptable Use of the College Network

The College provides students with computer facilities to facilitate learning and communication. When accessing network facilities students are expected to:

- log in using their own username and password;
- keep their password confidential at all times;
- be polite, considerate and use appropriate language;
- use equipment only for school related activities;
- treat equipment with care and respect;
- maintain the Standard Operating Environment (SOE) described below;
- keep the equipment clean and in good working order;
- report faulty or damaged equipment immediately;
- ensure material stored, used or accessed via a notebook or desktop on the Home Drive, Hard Drive or any external storage devices (eg, USB) regardless of whether the computer/notebook is connected to the College Network is legal, appropriate and in accordance with the *Student ICT Systems Acceptable Use Policy and Procedure;*
- log out of the College Network if leaving the computer or notebook unattended or at the end of each class;
- be responsible and accountable for actions which occur under their network account;
- adhere to the *Student ICT Systems Acceptable Use Policy and Procedure;*
- abide by all other relevant College policies.

3. Prohibited Use of the College Network

Students must not:

- use another students notebook;
- use or access another person's network account, email account, etc;
- give their passwords to anyone;
- use cloud accounts which are not associated with the college.

Under no circumstances shall the College's computer network be used inappropriately, including:

- to alter, re-configure, interfere with, mistreat or damage equipment;
- to depart from the Standard Operating Environment (SOE) provisions described further in this policy;
- to access or transmit any material that is defamatory, offensive or obscene (eg, violent, racist, sexist, pornographic) or in violation of any law or government regulation (eg, equal opportunity regulations);
- to breach copyright;
- in connection with the violation or attempted violation of any laws;
- to attempt to penetrate computer or network security of the College or any individual, company or other system;
- the contravention of the *Student ICT Systems Acceptable Use Policy and Procedure*;
- unauthorised access (or attempted access) to any other person's computer, network account, email accounts or equipment;
- to inappropriately access, attempt to access, or reveal College classified or confidential information;
- to be in breach of any other College policy.

This list should not be taken as exhaustive. The onus is on the individual student where doubt exists to seek advice and clarification from their Head of House/Head of Campus.

Viruses

Students must take reasonable steps to ensure that they do not introduce or propagate computer virus infections within the College community. Such reasonable steps include:

- ensuring that the computer they use has current virus definition files installed;
- regularly (at least monthly) conduct a full scan of their computer's hard disc drive;
- regularly scan any memory keys or CDs/DVDs used for transporting or distributing files;
- not opening files from insecure sources or sources where security is unknown or questionable;
- only opening email attachments that are expected or from trusted sources;
- not opening email that is of a questionable or dubious origin.

4. Monitoring

The College reserves the right to monitor and log the use of its computer facilities and to take appropriate action where use is a breach of College policies, poses a threat to security, and/or damages the College's reputation.

Student use of College computer facilities must be related to school work. Access to and time spent using many of these facilities is automatically logged.

Students and their families can have no expectations of privacy in relation to the use of College notebooks and the College's Network.

5. Standard Operating Environment

While most of the information below relates to the Standard Operating Environment of student notebooks, where appropriate it also applies to College desktop PCs.

Computer name
You are not permitted to change the computer name.

Administrator privileges
A student's notebook administrator password is available from the Notebook Service Centre. This set of privileges is necessary to install authorised (as set out in and in accordance with the Terms and Conditions for Student Use of College Owned Notebook) software and configure peripheral devices. Students must not use their administrator privileges to alter other aspects of the computer's configuration. If the configuration is changed and requires attention from Notebook Service Centre, staff will restore the default configuration of the notebook and a $20 service fee will be charged to the student and parent/guardian.

Peripherals
Students are welcome to connect home printers, digital cameras, scanners and other peripheral devices to the notebook. However, they should check that the device is compatible with Windows 8.1/10 and has an appropriate signed driver. If you have any concerns, please contact the Notebook Service Centre for clarification or assistance.

Backgrounds and Themes
The College uses the standard Windows theme. Students are permitted to change this setting and apply other themes to add a bit of personality to the device. This can make the device more welcoming to use. Any backgrounds and themes should be appropriate for display within a Catholic College Environment. Any background or theme should not hinder the ability to work on the device or consume excessive battery or processor power. The mouse cursor must be one of the standard (arrow type) mouse cursors.

If a staff member requests that you change your current theme due to it not being appropriate, hindering your ability to work or consuming excess resources on the computer then you must comply with this request. Notre Dame College staff have the final say on what background images and themes are appropriate. This must be respected or disciplinary procedures accordance with the College's Student Welfare and Discipline Procedures will be put in place. These will include the Notebook being swapped back to the standard theme and the ability to change the theme and background removed. This privilege maybe removed as part of disciplinary procedures.

File system shares
Students are not permitted to create any file system shares.

Peer to Peer (P2P) Networking
Installation of p2p clients such as Limewire, BitStream, BitTorrent, iMesh, WinMX or BearShare or like programmes is prohibited.

Ad hoc Wifi
Although your wireless network interface can operate in ad hoc mode (client to client), the standard configuration is AP mode (access point). Students are not permitted to change these settings. If students need to move files from one PC to another, they should use a USB memory stick or share via college provided cloud drive service.

Wireless Hotspots
Students are prohibited from setting up wireless hotspots for use with their notebooks to bypass the college network. Should a hotspot be detected in the college the equipment used to the setup the network will be confiscated for a period 7 days.

Mail Services
Students can send and receive email. Students are not permitted to send mail to groups of users within the College; ie addressing a message to "All Notre Dame College Staff" or "All Year 10's" etc, is not permitted. All emails sent or received via College mail servers are scanned by content filtering software.

Music, photographs, pictures and movies
Students are permitted to have these files on the notebook. These files must comform to the College's *Student ICT Systems – Acceptable Use Policy and Procedure*. Please note the Copyright Act prohibits users from storing music, images (photos and pictures) and movies, etc which are under copyright (meaning the music, images and movies, etc are owned by others).

Playing CDs or music files at school
Students are not permitted to play CDs or music files during class time unless specifically requested to do so by the teacher for a particular learning activity.

Games
Students are not permitted to install or play games on notebooks or College desktop PCs, regardless of if the games are website based or run from external media such as CDs, USB, hard drives or other.

Installation of additional software
Students are only permitted to install authorised software on the notebook computer.

Media Players
The notebook SOE includes Windows Media Player, iTunes and VLC Player.

Web Browser
College notebooks have Microsoft Edge/Internet Explorer and Google Chrome browsers installed. Setting Google Chrome as your default is recommended, use and installation of other browsers is not permitted.

Webcams
Student notebooks are equipped with webcams. Students are only permitted to use this feature of the notebook at school if:

- You have the permission of your supervising teacher;
- The use of the webcam relates specifically to your school work;
- You have the express consent of all individuals who will appear in any images or video created using the webcam; and
- Images or video taken with the webcam conforms to the College's *Student ICT Systems Acceptable Use Policy and Procedure.*

SECTION B - Electronic Communications

"Electronic Communications" refers to all equipment and forms of communication used to electronically communicate with others. This includes, but is not limited to the following:

- Email
- Instant Messaging
- Internet/Intranet
- Colleges Learning Management System
- Chat rooms/programmes/discussion boards and groups
- Video conferencing
- Web cam
- Social networking sites eg, Facebook, Twitter, blogs, wikis etc.

1. Acceptable Use of Electronic Communications

The College recognizes that electronic communication tools, when used appropriately and in accordance with College policies and rules can enhance student learning.

2. Prohibited Use of Electronic Communications

Students must not:

- use or access another person's network or email account;
- give their passwords to anyone.

Under no circumstances shall students use electronic communications inappropriately including:

- In a way that may be considered offensive, defamatory, obscene, pornographic, discriminatory, insulting or disruptive to any other person (*for example, pictures of naked people, semi clothed people, personal comments about students, staff or others, whether they are the recipient of the message or not).*
- Impersonate another identity.
- Post images, content, messages about Notre Dame College, its staff or students unless you have permission from Notre Dame College or the person(s) involved.
- To access, view, download, print or send messages or attachments (including to your home E-mail address), which include:
    - Language that is not appropriate in the College (such as swearing or sexually explicit references);
    - Sexually explicit messages or pictures;
    - To harass, intimidate, threaten or bully;
    - Offensive or inappropriate cartoons or jokes;
    - Unwelcome letters, suggestions, requests or propositions;
    - Ethnic or racial comments;
    - Any material which contains disrespectful comments about people with disabilities, or people's sexual orientation, or any person's physical attributes;
    - Sending chain mail;
    - Gambling;
    - Participating in online games (unless directly authorised by your teacher);
    - Joining a chat group;
    - Accessing social networking sites such as Facebook, My Space, etc (unless directly authorised by your teacher);
    - Breaching copyright laws including but not limited to software, database files, documentation, pictures, music, video, articles, graphic files, text or other downloaded information;
    - In connection with the violation or attempted violation of any laws;
    - For intentional dissemination of any computer viruses;
    - For personal advertising or for personal profit making;
    - To penetrate or attempt to penetrate computer or network security of the College or any company, system or individual;
    - For sending, forwarding, printing or receiving any material or data which does not comply with the College's rules and regulations
    - For collecting, storing or disseminating personal information or sensitive information *(including personal information or an opinion about an individual's racial or ethnic origin, religious beliefs or affiliations, philosophical beliefs, health information, criminal record, etc).*

This list should not be taken as exhaustive. The onus is on the individual student where doubt exists to seek advice and clarification from their Head of House/Head of Campus.

Please note:
Your intention in writing or sending a message is irrelevant. If a message offends, humiliates or intimidates another person it may breach this policy and relevant government legislation.

The College and/or individuals may be held liable for the content of messages which are offensive. Copies of electronic communications may be requested by external tribunals as discoverable documents if a complaint of harassment or discrimination is made against the student or the College.

3. Receipt and Transmission of Electronic Messages

The College understands that students cannot always control the messages that are sent to them.

The College employs industry standard content filtering software to minimize the transmission of offensive or nuisance messages. Nevertheless, the potential exists for inappropriate messages to be received by students (from both internal and external sources)

If a student receives an electronic message which they consider is inappropriate or contains inappropriate material and/or the message is in breach of the College's *Student ICT Systems Acceptable Use Policy and Procedure* and/or other College policies or rules, the student must:

- advise their teacher of this immediately;
- show the teacher the message;
- delete the message as instructed by the teacher;
- discourage friends, family, work mates etc from sending inappropriate electronic messages;
- Send a return electronic message which indicates that such messages should not be sent. For example the following could be sent:
  "Please do not send me this type of message again. The contents of this electronic communication do not comply with the College's Student Information, Communication and Technology (ICT) Systems Acceptable Use Policy and Procedure. In sending me this electronic communication, you are breaching the College's policies and putting me at risk of doing so. A breach of the Student Information, Communication and Technology (ICT) Systems Acceptable Use Policy and Procedure has serious consequences."

Students must not:

- forward the electronic message or the material contained in the message to anyone else;
- print or distribute the message/material by any other means.

4. Monitoring Electronic Communications

Access to the College's computer network is a privilege not a right. All students should be aware that:

- the content of electronic communications is monitored by the College to ensure compliance with this and other policies and to support operational maintenance, auditing and security activities.
- all electronic communications and attachments to electronic communications stored on the College's computer system and notebooks are the College's property and may be viewed by the College.
- all electronic communications and internet transactions and communications may be monitored or intercepted by other parties (*including parties other than the College*).
- students and their families can have no expectations of privacy in relation to electronic communications.

SECTION C - The Internet

The College understands that web 'surfing' may be related to students' legitimate studies but the potential for abuse exists. The College encourages exploration of the Internet for legitimate study related activities.

1. Appropriate Use of the Internet

When surfing the internet students must

- Report to their teacher any site that they may have accidently accessed which has inappropriate material so it can be blocked. Provided students follow this procedure there will be no disciplinary action against the student.
- Regularly change their password to ensure the security of their account (monthly is recommended).
- Ensure their password remains confidential at all times.
- Be responsible and accountable for all actions under their account log in and password.
- Use the internet in accordance with the *Student ICT Systems Acceptable Use Policy and Procedure.*
- Abide by copyright laws.
- Use the internet for educational purposes only when using college equipment or college services.
- Students must agree to and abide by Google Apps for Education Acceptable use policy/Microsoft Terms of Use If students do no abide by these polices their account may be terminated by Notre Dame College or the service provider. A termination of account will result in disciplinary procedures.

2. Prohibited Use of the Internet

When surfing the internet students must not:

- Access sites which maybe offensive. This includes, for example, racist, sexist, pornographic or violent material.
- Reveal their or other peoples personal details, including for example, personal or email addresses, phone numbers, or photographs of individuals etc.
- Login or attempt to login using anyone else's account username and password.
- Access or download any information from the internet which contravenes the *Student ICT Systems Acceptable Use Policy and Procedure* or any other College policies or rules.
- Download any information which poses a security risk (eg, viruses).
- Take part in an action which breaks the terms and conditions of the site/service they are using. For example age restrictions or posting inappropriate content.

This list should not be taken as exhaustive. The onus is on the individual student where doubt exists to seek advice and clarification from their Head of House/Head of Campus.

3. Access to Cloud Services

Notre Dame College provides a range of cloud services, these are to be used for only college/educational related activities. Use of these sites for storing personal files/information/programs/games is prohibited. Notre Dame College reserves the right to actively remove content without warning for items which are not deemed appropriate to the college. A discretionary charge of $20 will be applied when cleaning up cloud service accounts.

4. Sharing

When using cloud services there will be facilities to share content with other users, these users could be either internal or external to the college. Students should not share content with other users unless permission has been given by their classroom teacher and only with the users permitted by teacher. Sharing unsolicited content with other users is prohibited and will result in disciplinary action.

5. Monitoring of the Internet

- The College employs industry standard content filtering software to minimize access to offensive and inappropriate sites. Nevertheless the potential exists for students to access inappropriate sites. Students must follow the procedure outlined above in 'Appropriate Use of the Internet' if this occurs.
- The content of internet communications is monitored by the College to ensure the compliance with College policies and to support operational maintenance, auditing and security activities.
- All internet sites accessed are tracked and logged and may be viewed by the College.
- All internet transactions may be monitored or intercepted by other parties (including parties other than the College).
- Students and their families can have no expectation of privacy in relation to internet usage.

The Notre Dame College will complete audits of cloud service accounts it provides, students found with content considered not college/education related, personal, breaking copyright, breaking cloud provider's terms of use or illegal could be removed without warning by college staff. Audits will be carried out randomly or when requested by a member of staff. They will be completed without warning and offending content will be documented, reported and may be removed followed by disciplinary action. Inappropriate content found to be shared will other members of the college could result in the recipients of the content also being audited. A discretionary charge of $20 will be applied when cleaning up cloud accounts. If you received content which you consider inappropriate you should advise your teacher, show your teacher and delete the content if requested. You can discourage your friends from sharing inappropriate content by responding to the shared content with a message similar to:

Please do not share this type of content with me again. The contents of this electronic communication do not comply with the College's Student Information, Communication and Technology (ICT) Systems Acceptable Use Policy and Procedure. In sending me this electronic communication, you are breaching the College's policies and putting me at risk of doing so. A breach of the Student Information, Communication and Technology (ICT) Systems Acceptable Use Policy and Procedure has serious consequences."

SECTION D

Breaches of the *Student ICT Systems Acceptable Use Policy and Procedure*

Breaches of this policy by students are considered to be serious. In some cases a breach may expose the student, their family and/or the College to legal liability and in extreme cases criminal prosecution.

Where a student has breached this policy they will be dealt with according to the College's Student Welfare and Discipline Procedures. This may result in:

- Immediately removing the students access to any part of the College's Network/Cloud services;
- Removing the ability to change the background and theme of the notebook;
- The removal of the notebook from the student;
- Audit and review of all material viewed on, sent to and from the Network by the student;
- Taking disciplinary measures against the student;
- Where there is a reasonable belief that illegal activity may have occurred the College will report the suspected illegal activity to the police.