Belfast Bible College's I.T. Student Acceptable Use Policy

Scope and Purpose	This process applies to all students enrolled at Belfast Bible College, and anyone who has access to a College computer network.
Implication of non-adherence	Breach of Data Protection Act 1998 and/or Computer Misuse Act 1990
Compliance and Regulatory requirements	To comply with Computer Misuse Act and Data Protection Act
Who uses the process	All students and those with access to Belfast Bible College computer network including Moodle VLE, email or social media, or use College IT facilities.
Roles and Responsibilities	College IT Officer has responsibility to monitor the network to ensure compliance
Process review	This process should be reviewed following the end of each academic year
Date last reviewed	June 2022
Date next review	June 2023

Summary

The College is pleased to offer students access to the organisation's computer Network and the Internet. This Policy applies to students granted Network and Internet access by the College. It also includes the College's Office 365 system, College applications facilitating online learning (Including Moodle – the College's VLE) and social media opportunities, and applies to their use at the College's campus, as well as at remote locations, including but not limited to students' homes. These rules and policies apply to all full-time students and part-time students. Any student who violates the College's e-mail rules and policies will be subject to disciplinary action, as per the Disciplinary Process.

For the College to continue making Network, Internet access, and the other IT opportunities available, students must behave appropriately and lawfully. Upon acceptance of your account information and agreement to follow this Policy, you will be granted Network and Internet access. If you have any questions about the provisions of this Policy, you should contact the Communications Manager.

If you or anyone you allow to access your account (itself a violation of this Policy) violates this Policy, your access will be denied or withdrawn until disciplinary process has been completed.

1. Personal Responsibility

By accepting your account password and related information, and accessing the College's Network or Internet system, you agree to adhere to this Policy. You also agree to report any Network or Internet misuse to the Communications Manager.
Misuse includes Policy violations that harm another person or another individual's property.

2. Term of Permitted Use

Network and Internet access extends throughout the term of your study provided you do not violate the organisation's I.T. Acceptable Usage Policy. Note: The College may suspend access at any time for technical reasons, Policy violations, or other concerns.

3. Purpose and Use

a. Network

The College offers access to its Network and Internet system primarily for study purposes but does permit appropriate personal use.

The College Network and Internet connection may not be used directly by any user for the download, creation, manipulation, transmission or storage of:

- any offensive, obscene or indecent images or pornographic material.

- unlawful material or material that is defamatory, threatening, discriminatory, extremist.
- material which is subsequently used to facilitate harassment, bullying and/or victimisation of anyone.
- material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation.
- material with the intent to defraud or which is likely to deceive a third party.
- material which advocates or promotes any unlawful act.
- Emails containing unknown attachments or downloading malicious software to a College computer or on the College network.

Any user found to be in breach of any of these terms will have their access to the network revoked and may face disciplinary / legal action by the College.

b. Online applications including Office 365 & VLE (Moodle)

The College provides each student with a licence to use Office 365 and any of its associated tools, as well as allowing access to and use of, the College VLE (Moodle), solely for study purposes in relation to the academic programme you are registered on, and general education related information provided by the College. Students are **not** permitted to share, copy or use materials or resources hosted on the College VLE except for their studies while enrolled as College members. Students are forbidden to share their personal logon, or to use someone else's logon to access any aspect of the College's online applications.

c. E-mail.

The College allows e-mail access primarily for the purposes of study and communicating College information. Students may use the College's e-mail system for personal use only in accordance with this policy, such as to communicate with family members and friends, however, students are prohibited from using e-mail to operate a business, solicit money for personal gain, campaign for political causes.

Students are prohibited from using e-mail to engage in activities or transmit content that is harassing, discriminatory, menacing, threatening, obscene, defamatory, or in any way objectionable or offensive.

d. Social Media

Students are personally responsible for anything they post on social media. They should assume that everything they post online will be public and permanent regardless of any privacy settings they assume are applied. Many of those operating social media sites specify that they have an irrevocable and permanent license to use and distribute the content posted to their sites and for any purpose. Students should be aware that the content of social media may easily become available to the public, including the College staff and the media and that inappropriate use could result in disciplinary proceedings or damage their reputation or future career prospects.

Adhering to the following simple rules should help to avoid some of the most common pitfalls.

Social Media should not be used to post a complaint about any aspect of College life, whether academic or non-academic. Complaints should be taken up in accordance with the College's complaints policy in which case they will be handled appropriately.

Social media should not be used by students to make any derogatory remarks about an individual, group, organisation or to insult another person's beliefs. Social media should not be used to post images or videos that would bring harm or embarrassment to another person or bring the College into disrepute.

Should any group wish to set up a social media site that in any way affiliates itself with the Belfast Bible College, that group must have the permission of the College and state on the site that the views expressed are not necessarily those of the College; the group becomes

responsible for maintaining the site and ensuring its content is appropriate and in line with the policy outlined above.

Belfast Bible College reserves the right to monitor any social media sites that affiliate themselves with the College and, where necessary, to request the removal of sites that reflect negatively on the College. Students and staff should also report to a member of staff (ultimately the Communications Manager), if they become aware of any inappropriate content which is related to the College.

- Also know who you are engaging with, and do so appropriately
- Do not engage in any conduct or behaviour or language that would bring the College into disrepute. Individuals should exercise caution when interacting with, and responding to, potentially contentious posts on social media sites that may bring the College into disrepute.
- Take particular care when dealing with content relating to children or vulnerable adults; if this is necessary then best practice should be followed and permission should always be sought from College staff.
- Be thoughtful and polite; before sending, think about how others might respond to your communication and the consequences of it.
- Adhere to the advice in this policy when undertaking work placement or paid work or any other duty on behalf of the College but also ensure compliance with the employer's policy.
- Look out for security threats - be on guard against phishing attempts or other attempts to corrupt your account.
- Students need to consider intellectual property rights, copyright and ownership of data when using social media.

e: Video Conferencing

- What is videoconferencing?

  Videoconferencing is a means by which a student, in certain circumstance, can complete a course unit without being physically present in the class. It involves synchronous two-way audio and video engagement, using an agreed videoconferencing platform, and is designed to allow a student to be an active participant in a class.

- What can I expect?

  While videoconference can be used to help students engage in classes from a distance, it is not the same experience you would get if you sat in the physical classroom. Students undertaking a class by videoconference need to be aware that at times they may struggle to hear the discussion throughout the room and may find it difficult to read notes written on the board. While discussion can take place via videoconference, this is generally not as easy as face-to-face discussion. Videoconference is not the same experience as attending a class in person.

- Who is allowed to video conference classes?

  This option is not available to all students, at all times, or for all classes. It is intended to support students who, for reasons beyond their control, are unable to attend class in person. The Academic Office determines who is able to access video conferenced classes.

- Etiquette for videoconference:

  When you are participating in a videoconference class (two-way audio and video), you appear on a screen near the lecturer in the room, and it is helpful to be aware that your movements can be seen by the class. Because of this, we ask students who are videoconferencing to follow the following etiquette guidelines:

  - If there are noises in the background at your location, please mute your microphone until you are ready to speak, and re-mute it afterwards.

- Please do not get up and leave your computer until the class break (whenever possible).
- Please close the door to your room, to avoid other people coming on camera and distracting both you and the class.

4. Online Etiquette Rules

Students must adhere to the rules of Online Etiquette, in other words, you must be polite, adhere to the organisation's electronic writing and content guidelines, and use the Network, Online applications and Internet appropriately and legally. The College will determine what materials, files, information, software, communications, and other content and activity are permitted or prohibited, as outlined below.

Violations - These guidelines are intended to provide College students with general examples of acceptable and unacceptable use of the College's system. A violation of this policy may result in disciplinary action.

5. Banned Activity

The following activities violate the College's I.T. Acceptable Usage Policy:

(A) Using, transmitting, receiving, or seeking inappropriate, offensive, vulgar, suggestive, obscene, abusive, harassing, belligerent, threatening, defamatory (harming another person's reputation by lies), or misleading language or materials.

(B) Revealing personal information, such as the home address, telephone number, or financial data of another person or yourself.

(C) Making ethnic, sexual-preference, or gender-related slurs or jokes. Engaging in illegal activities or encouraging others to do so. Examples:

- Accessing, transmitting, receiving, or seeking unauthorised, confidential information about students or staff.

- Conducting unauthorised business.
- Viewing, transmitting, downloading, or searching for obscene, pornographic, or illegal materials.
- Accessing others' folders, files, work, networks, or computers.
- Intercepting communications intended for others.
- Downloading or transmitting the organisation's confidential information.

(D) Students must not use social media or email for any of the following under any circumstances:

- To represent the College without the express written consent of a member of staff
- to post inappropriate, discriminatory or defamatory comments including comments about other students, staff, or work placement employers or their clients
- to bully, harass or intimidate other students, staff or members of the public
- to post threatening, obscene or profane comments
- to express or support sexist, racist, sectarian or homophobic views
- to express support for illegal activities or organisations
- to disseminate misleading information
- to share confidential or sensitive information
- to view or distribute sexually explicit or offensive content
- to infringe or violate someone else's rights
- to post personally identifiable information that could be used to locate any individual without that person's permission
- to post content that could create a security risk for the College or its staff or students
- post anything which, in any way, may be unlawful

(E) Causing harm or damaging others' property.

Examples:

- Downloading or transmitting copyrighted materials without permission from the copyright holder. Even when materials on the Network or the Internet are not

marked with the copyright symbol, ©, students should assume all materials are protected under copyright laws—unless explicit permission to use the materials is granted.

- Using another student's password to trick recipients into believing someone other than you is communicating or accessing the Network or Internet.
- Uploading / Downloading a virus, harmful component, or corrupted data. Vandalising the Network.
- Using software that is not licensed or approved by the College.

(F) Jeopardising the security of access, the Network, or other Internet Networks by disclosing or sharing passwords and/or impersonating others.

(G) Accessing or attempting to access controversial or offensive materials. Network and Internet access may expose students to illegal, defamatory, inaccurate, or offensive materials. Students must avoid these sites. If you know of students who are visiting offensive or harmful sites, report that use to the College's Communications Manager.

(H) Wasting the College's computer resources. Specifically, do not waste printer toner or paper. Do not send electronic chain letters. Do not send e-mail copies to nonessential readers. Do not send e-mail to group lists unless it is appropriate for everyone on a list to receive the e-mail. Do not send organisation-wide e-mails without the Communications Manager's permission.

(I) Encouraging associates to view, download, or search for materials, files, information, software, or other offensive, defamatory, misleading, infringing, or illegal content.

6. Privacy

Network, Online applications and Internet access are provided as a tool for student study. The College has the legal right to monitor usage of the Network, Online applications and Internet access, using the least intrusive method available. When monitoring is deemed

necessary, students who are being monitored will be notified of the College's decision to monitor, will be provided with details of what is being monitored, why and how. All Internet use is continuously monitored.

8. Fair Usage

The broadband to the College is limited by speed and bandwidth and so has to be shared across the campus and all users. This may at times mean that access is limited or slowed to allow for more people get access. If anyone is using excessive amounts of broadband to download or stream large amounts of data then their access will be initially restricted and a warning issued. A subsequent offence will result in the termination of their access to the network.

9. Non-compliance

Your use of the Network, Online applications and Internet access is a privilege, not a right. Violate this policy and, at minimum, your access to the Network, Online applications and Internet access will be restricted, perhaps for the duration of the remainder of your study with the College. Policy breaches include violating the above provisions and failing to report violations by other users. Permitting another person to use your account or password to access the Network, Online applications and Internet - including but not limited to someone whose access has been denied or terminated - is a violation of Policy. Should another user violate this Policy while using your account, you will be held responsible, and both of you will be subject to disciplinary action.