ST BRENDAN'S
SIXTH FORM COLLEGE

Faith in Learning

IT Acceptable Use Policy

Revision number	202501
Reviewed by	IT Infrastructure and Technical Manager
Next review date	March 2027
Policy owned by:	Executive Finance Director

Introduction

The College provides IT equipment and services for is normal operations. This Policy sets out the responsibilities of users in regard to how those services and devices are used and accessed. Users are required to sign a copy of this Policy as evidence that they have read and understood the conditions herein and that they agree to comply with the Policy in its entirety.

Scope

This policy applies to any person accessing the College's IT systems or data platforms

1. General Points

1.1. The College reserves the right to monitor all aspects of its telephone and computer systems that are made available, and to monitor, intercept and/or record any communications made by network users, including by telephone, e-mail, local-area-network or internet communications.

1.2. By reading a copy of this Policy Document within their National College Account all users consent to Clause 1.1 above in accordance with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

1.3. Computers and e-mail accounts are and remain the property of the College and are provided for the performance of College work only. Any communication using the College's systems covered by this Policy of a personal or private matter shall not be treated differently to College related communications and therefore shall not be subject to privacy rights beyond those of employment contract or Data Protection rights as Data Subjects of the College engaged in College business.

1.4. Network users must not access, download, or transmit any material, which might reasonably be considered obscene, abusive, sexist, racist, or defamatory. This includes material that may be contained in "jokes" sent by e-mail. Misuse of network systems will be treated as misconduct and will be subject to disciplinary procedures. The College reserves the right to use the content of any network user's e-mail, internet 'history' or network usage in any disciplinary process.

2. Examples of Un-acceptable use:

2.1. Corrupting or destroying other user's data

2.2. Violating the privacy of others

2.3. Disrupting the work of other users

2.4. Using the network in a way that denies service to others, e.g., deliberately overloading of printing facilities, deliberately overloading of access links (Internet link), and excessive downloading without prior authorisation from IT.

2.5. Deliberate or thoughtless introduction of a malware into the network environment

2.6. Installation of unauthorised software on college machines

2.7. Defamatory remarks in electronic communications

2.8. Downloading, storing or transmitting any material, which might reasonably be considered obscene, abusive, sexist, racist, or defamatory.

2.9. Any attempts to disable, defeat or circumvent any of the College's computer security facilities

2.10. Intentional physical damage to college devices

3. Electronic Communication

3.1. Any electronic communication (including, but not limited to, e-mails, blogs, tweets, wikis, instant messaging and text messaging) should be drafted with care. It should be remembered that it is a permanent form of written communication and can be recovered even after it has been 'deleted'. Network users should ensure that the content and tone of all communications (both within and without the College community) are of a professional standard and uphold the good reputation of the College.

3.2. Communication of material which might be regarded as sexually explicit or offensive on grounds of equality, diversity and inclusion, or which could bring the College into disrepute, will be regarded as a disciplinary matter

3.3. The College's communication platforms are for College business only – the sale of personal goods, advertising and/or anything else that does not directly related to College business is prohibited. Noncompliance with this clause may be treated as misconduct.

3.4. Network users should not make derogatory remarks in communications about other persons. Any written derogatory remark may constitute libel.

3.5. Network users may want to obtain confirmation of receipt of important messages. Network users should be aware that this is not always possible and may depend on the external system receiving the message. If in doubt, telephone to confirm receipt of important messages.

3.6. By sending messages via the College's systems users are consenting to the processing of personal data contained within. If users do not wish the College to process such data, they should communicate it by other means.

3.7. The College blocks all potentially executable attachments, since these types of files potentially constitute the most severe virus or malware risk.

4. Internet

4.1. The College monitors all Internet access and blocks access to sites with unsuitable content. Network users should not assume that just because a site is not blocked that the College does not consider it unsuitable. Sites that contain inappropriate material must not be accessed. Accessing sites with inappropriate material may lead to disciplinary action. The College expects all College network users to report any sites containing inappropriate material that can be accessed to IT so that the site(s) can be blocked.

4.2. Intentional access to any material or website which might be regarded as inappropriate under the College's Equality Diversity and Inclusion Policy or as harassment under the Equality Act 2010, including sexually explicit or offensive materials relating to race, gender, sexual orientation, transgender, age, religion or disability issues may be regarded as gross misconduct and, as such, subject to disciplinary action.

4.3. Reasonable private use of the Internet is permitted but should be kept to a minimum and should not interfere with work. Excessive private use of the Internet during working hours may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct. The college tracks and filters all outgoing and incoming internet traffic.

4.4. The College reserves the right to withdraw, at any time, access to social networking sites or personal blogs on college managed networks.

4.5. If the Internet facilities are used for personal use, such as purchasing goods with a credit card, users do so at their own risk. The College accepts no responsibility for any personal transactions carried out over the College network.

5. User Accounts

5.1. Passwords for College systems must comply with the College's password policy
5.2. Users are responsible for safeguarding their passwords. Passwords should only be documented where they can be securely stored (Password Managers, Lockable cabinets / lockers)
5.3. Passwords must never be printed, or revealed to anyone, including those who have authority over you and the IT Team.
5.4. Extreme caution should be exercised when opening communications that ask for network credentials and or contain links to unknown websites.
5.5. If users suspect that their account has been compromised, they should change their password immediately and contact IT Support
5.6. On and before leaving the College it is the user's responsibility to ensure that any electronic documents to be retained are transferred as appropriate and in line with College procedures
5.7. A user network storage areas (e.g OneDrive / H:\) is primarily for storing items that relate to College work; it is not for personal use. Using this area to store personal items may lead to disciplinary action.

6. Ownership & Investigations

6.1. Managers/teachers do not have automatic rights to access the data of another member of staff or student. If a manager or a colleague needs access data when the data owner is absent or on leave, they must seek authority via the IT Team giving precise details about the data that needs to be accessed. The whole process will be recorded and, in all cases, reasonable attempts made to contact the data owner request permission or advise them of the action being taken out. Requests need to be made via IT Helpdesk ticketing, and will be subject to normal prioritisation.
6.2. Any breach or perceived breach of this Policy must be investigated. In the first instance any investigation must be discussed with either HR or Student Services (as appropriate) before contacting IT. Checks will be made by IT only after approval by either the IT Infrastructure and Technical Manager or the Vice Principal when the subject is not asked for consent.

7. Security and Networks

7.1. Ability to connect to other computer systems through the network does not imply a right to connect to those systems or to make use of those systems unless authorised to do so. Users should not alter or copy a file belonging to another user without first obtaining permission from the creator of that file.
7.2. Whilst away from their device, users must ensure that they are either logged off, or that their device is locked
7.3. The college supports the use of personal devices to access the college network and provides a dedicated wi-fi network to do so. By connecting to these networks, users will be deemed to consent to be bound by the College's BYOD policy.
7.4. All College related data should be stored wherever possible on the College Network drives in order for it to be included in the daily backup routines.
7.5. Any data stored directly on the PC's hard drive and other storage devices (i.e. Pen drives and external hard drives) is the responsibility of the user and therefore own backup routines should exist and be implemented.

8. Copyright & GDPR Infringement

8.1. Copyright applies to all text, pictures, video, and sound, including those sent by e-mail or on the Internet. Files containing such copyright protected material may be downloaded, but not forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate.
8.2. Copyrighted software must never be downloaded. Such copyrighted software will include screen savers.
8.3. Users of the computing facilities should not import non-text files or unknown messages on to the College's system without having them scanned for viruses.
8.4. Storing files for personal use (i.e. MP3/4 files, Wedding Photos) on College IT equipment is strictly prohibited and any such files will be removed without notice.
8.5. The installation of officially recognised licensed Software must be authorised and carried out by the IT Team or an approved external agency as appropriate.
8.6. The use, or possession, of unlicensed copies or "pirated" versions of software is illegal and, therefore, strictly prohibited.
8.7. Installing unauthorised software may lead to disciplinary action and may in some circumstances be treated as gross-misconduct.
8.8. Users of the College will be subject to the rules and regulations laid down in the College's policies and procedures relating to GDPR and Information Security.

9. College owned mobile devices – laptops, mobile phones

9.1. Users of the College's mobile devices must be vigilant in regard to cyber security. If a device is stolen, the user is expected to report the theft to the police, obtain an incident number and contact IT Support as soon as is possible.
9.2. Users of the College's mobile devices must not change technical settings or interfacing configurations of laptops or other equipment without first consulting IT Services. Users who alter the configuration of a device, may be liable to compensate the College for any losses.
9.3. Users who are loaned equipment are required to sign for it and bear the responsibility for its care. Loan equipment should be concealed and stored securely when not in use.

10. Social Media

10.1. The College provides internet access for College, but the College recognises that the internet may be used for personal reasons, and that that may include social networking on websites such as Facebook and X (formerly known as Twitter). However, all members of the College community are expected to always set the highest professional standards, both in and out of college, in order that the College achieves its Mission and that the reputation of the College is safeguarded. Users must maintain a separation of social media accounts between those for solely College and those for personal/ business use.

10.2. The use of social networking sites or personal blogs (online diaries), must not include any references to the College that could bring it into disrepute. Nor must any reference be made to individuals connected with the College, which may be construed as harassment. The College will treat any breaches of this clause as a disciplinary matter.

10.3. All network users must take care not to allow their input on social media websites to damage working relationships between members of the College's community. Postings to newsgroups of social network sites are in effect e-mails published to the world at large and are subject to the same regulations governing email as above. It is expected that disclaimers are used in a posting if it could be interpreted as an official statement or policy or opinion of St Brendan's Sixth Form College. A disclaimer could read, for example: "The views expressed are my own and do not necessarily represent the views or policy of the St Brendan's Sixth Form College..." If a user makes a remark or is responsible for or is in any way involved with posting material which in the opinion of the College brings the College into disrepute or otherwise damages the College's interests, disciplinary action may also be taken in line with the College's appropriate disciplinary policy. Any legal means may be taken to search accessible materials relating to the disciplinary action.

10.4. No endorsements about members of the College Community, or personal comments about members of staff and students are acceptable. If in any doubt about other specific usage of site(s) then discuss the matter with your Curriculum Leader/Line Manager or, in the case of students, your Academic Coach.

10.5. Network users must be security conscious and should take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. In addition, users should ensure that no information is made available that could provide a person with unauthorised access to the College's systems and/or data; and refrain from recording any confidential information regarding the College on any social networking website. Care should always be taken to ensure that information provided to such sites does not contravene our General Data Protection Policy.