ST BRENDAN'S
SIXTH FORM COLLEGE

Faith in Learning

IT Security Policy

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

Contents

1. Roles and Responsibilities

- The Executive Finance Director is responsible for this policy and its enforcement is the responsibility of the IT Infrastructure and Technical Manager.

- Only authorised persons have access and rights to the College's systems and information.

- The IT Infrastructure and Technical Manager will ensure that access to the College's information and information systems is restricted to authorised users only, and will maintain appropriate internal controls and processes to manage the set-up and access rights to email and information systems through user accounts.

- All users must comply with the College's IT Acceptable Use standard and Data Protection Policy. Failure to comply will lead to disciplinary proceedings and possible termination of employment.

2. Account Management

Account Eligibility

- User accounts who identity has been verified by the HR or MIS department will only be provided for;
  - permanent and fixed term employees and temporary staff;
  - students, applicants and parents;
  - staff from other organisations who provide services to the College and may require access to the College's information systems in order to fulfil their contractual obligations; and
  - non-human interfaces only where absolutely necessary, and subject to approval procedure and regular review.

- When an account is created, a unique identifier (User ID) will be assigned to the individual user for his or her individual use.

- Users will be allocated access rights in accordance with their role and responsibilities and the level of access required will be defined and authorised by their line manager or system application owner.

- Access to the main student records system will be monitored using an access privileges system and authorised by the MIS Team.

- Accounts will be monitored to identify any improper and inappropriate use of systems and services.

- Access rights will be adjusted appropriately and in a timely manner to reflect any changes in a user's circumstances e.g. when a member of staff changes their role or a member of staff or student leaves the College.

- Requests to be added to different groups, e.g. for access to staff shared areas, must come from the head of the department/system owner responsible or a member of the College Leadership Team (CLT).

User account conditions for use

- Account holders must comply with the following conditions:
  - Credentials (user ID and password) must not be given or shared to any other person, user or service.
  - A user ID may not be re-assigned to any person at any time (user IDs will not be recycled).
  - Users will only access systems using their designated account.
  - Users will logoff their accounts when not in use.

(Privileged) Administrative Account Management

- Privileged accounts have higher levels of access e.g. to systems settings.
  - These must only be used for system administration tasks and not for day to day transactions.
  - A written request from the application owner is required before privileged access is granted.
  - A record of all privileged account holders will be maintained by application owner; this will be reviewed at 6 monthly intervals or during relevant staff changes.
  - Any users who no longer need administrative access to carry out their role should have their access removed by the application owner.
  - Administrator accounts are not to be used to access websites or download email.
  - Software and update downloads should be performed by the application owner as a standard user and then installed as an administrator.

Account Creation

- Accounts must only be created where eligibility criteria are met.

- Student accounts will automatically be created as Pre-admissions accounts that will have an active directory and limited Microsoft 365 access, fully linked to the college MIS (Management Information Services) system.

- Pre-admission accounts will automatically be transferred to a student account when the user enrols and has ‘current’ status in the college MIS system.

- Parental accounts will be created when the student enrols and has ‘current’ status in the college MIS system.

- Group memberships within Identity Mangement systems (IDMs) will be assigned by the IT Services Department based on information provided on the new starter form.

- Temporary accounts maybe requested in circumstances, but will have restricted access; be fully documented; and deleted after use.

Ending of User Access

- Where a student leaves the College and is marked as a 'leaver' by the MIS team their system access account will be revoked.

- When a member of staff reaches their leaving date: (As notified by HR)

    - Any system access is revoked.
    - Access to email is removed and only recoverable for a brief period after this date.
    - Any backups of personal data should be completed before leaving the College.
    - Line managers of leavers are responsible for ensuring continuity of shard data and resources.
    - Application owners will ensure that accounts are disabled / removed when staff leave.

- Temporary accounts will be deleted when they are no longer required.

Account/Data Retention

- Unless user data has been appropriately classified in accordance in the College's Document Retention Scheme all 'Cloud' and on premises user account data will be retained for a maximum period of 90 days before deletion.

- It is not operationally feasible to ensure that user profiles stored on local machines is retained for a period of 90 days.

Password Management

- Password standards are in line with the current recommendations from the National Cyber Security centre for:
    - Password format and structure
    - A password change frequency

- The current criteria will be stated in the IT password policy.

- Passwords must be changed immediately by the user as part of the account set-up.

- Passwords should be kept secure and encrypted using a password manager, if they are required to be documented.

3. Connecting devices to the college network

- The following regulations apply to all College system users:
  - It is not permitted to connect private equipment to any network socket without the prior consent of the IT Infrastructure and Technical Manager.
  - Private equipment may be connected to the College's wireless networks.
  - Private equipment must not be connected to any College PC or laptop, irrespective of where the equipment is located.
  - Private storage devices (USB Sticks / HDDs) without encryption must not be used for any College related data.
  - Devices connected to the College network must have up to date applications including antivirus software.
  - Devices connected to the College network must be encryption enabled
  - Devices connected to the College network must be able to receive updates from the College's patching tool and have a supported operating system that is regularly patched.
  - Devices which are not managed effectively, will be disconnected from the network without notice

College owned devices

- The College may at times provide devices to some of its members either staff or students. When it does, it will supply devices which are appropriately configured to ensure that they are as effectively managed as devices which remain within the office environment.

- Devices supplied by the College must meet the minimum-security requirements as set by Cyber Essential guidance.

- In addition, the following conditions of use apply:
  - Non-members of the College (including family and friends) must not make any use of the supplied devices.
  - No unauthorised changes may be made to the supplied devices.
  - All devices supplied must be returned to the College when they are no longer required or prior to the recipient leaving the College, irrespective of how they were purchased. Failure to do this will incur the cost of the device being sought from the individual, either from their last wage payment (in the case of staff) or through official channels.
  - No attempt must be made to change the College's standard configuration including the configuration of anti-virus, policies, user rights, encryption, or system updates.
  - Appropriate mobile device management (MDM) will be applied to the relevant device through policy management to ensure devices are maintained, updated and in a secure state.
  - Procedures will be implemented to ensure that college devices are regularly updated, all college devices and servers will be updated with latest security patches on a fortnightly basis, or more frequently if serious flaw is discovered.

Portable IT Equipment

- Procedures will be implemented to protect against accidental damage, loss or misuse of portable IT equipment and the accidental disclosure of confidential or sensitive data. These will include;
  - An on-loan record will be maintained of equipment.
  - The security of portable equipment and any data contained or produced thereon will be the responsibility of the person to whom the equipment and / or data has been allocated.
  - Equipment will be stored securely, both on site and off site, and during transportation off site.
  - Where appropriate, virus protection software will be installed and updated at a frequency set by the IT Department.
  - Only authorised College staff will carry out repairs and modifications to equipment and updates to software.
  - Any on loan portable equipment will be recovered as part of the staff / student exit procedure.
  - A review of on loan equipment will be undertaken each term.

College Servers, Workstations, Laptops

- To ensure that all servers or workstations on College network are correctly installed and configured.
  - They will be installed by IT department staff according to correct procedures.
  - They will have appropriate security in place to ensure that data and services are protected.
  - They will have the relevant software and hardware correctly installed.
  - They will have up to date anti-virus software.
  - Laptops will have appropriate security in place including full disk encryption.

Personally Owned Devices (BYOD)

- The college will support and encourage the use of staff or student personally owned devices (bring your own device (BYOD)) and to use those devices to securely access the college's systems, applications, and information. This can mean using their own smartphones, tablets or laptops for college work.
  - Personally owned devices will not be permitted to join the college curriculum network.
  - A designated College Staff and Student network will be provided to ensure Cyber Essentials procedures and protocols are met for external visitors.
  - Wireless connectivity for network users is facilitated via authenticated College accounts
  - There will be clear expectations about the use of personal devices, and this will be communicated via the College BYOD Policy.
  - A yearly audit of staff personal devices will take place to ensure that devices comply with CE (Cyber Essentials).
  - Only devices that comply with CE's list of supported operating systems will be authorised.
  - Conditional access rules through Entra AD will be reviewed yearly to ensure mitigations are in place to reduce the risks to the college network.
  - Appropriate MFA will be applied as required.

Device Locking

- Where a device requires the physical presence of a user to gain access to the services the device offers (e.g. laptop logon, mobile phone unlock) the user must unlock the device using a credential such as a biometric, password or PIN (Alpha-Numeric) before gaining access to the services.

- Biometric tests, passwords and PINs must be protected against brute-force attack by at least one of:
  - 'throttling' the rate of attempts. This should permit no more than 10 guesses in 5 minutes.
  - locking devices after no more than 10 unsuccessful attempts

- Credentials that are solely used to unlock a device, a minimum password or PIN length of at least 6 characters must be used.

- When the device unlocking credentials allow access to college data or systems, then the password must meet College criteria set in the IT Password criteria policy.

Virus and Malware Protection

- Industry recognised anti-virus software will be installed and kept up to date across the College's computers.

- The frequency and level of virus checking will be as follows:
  - Each time a file is opened
  - Daily check at server level
  - All e-mail attachments prior to use
  - All files opened from external sources

- Only software authorised by the IT Infrastructure and Technical Manager and/or Executive Finance Director will be installed on college equipment.

- The use of unauthorised software will be prohibited.

4. Boundary firewalls and internet gateways

- Default administrative passwords should be changed in line with the administrative password criteria.

- Access to the administrative interface (used to manage firewall configuration) from the internet should be prevented, unless there is a clear and documented business need and the interface is protected by one of the following controls:
  - multi-factor authentication (see MFA details below)
  - an IP allow list that limits access to a small range of trusted addresses combined with a properly managed password authentication approach

- By default unauthenticated inbound connections should be blocked.

- Inbound firewall rules should be approved and documented by the IT Infrastructure and Technical Manager and/or Executive Finance Director with reference to the documented procedures in line with business case requirements.

- Firewall rules that are no longer needed should be removed quickly as possible.

Internet Access

- Internet access will be provided to all network users via their authorised network user identifier and password. Guests of the College will be accommodated upon advanced request.

- The Internet will only be used for college related work.

- Personal or College confidential information will not be transmitted across the Internet.

- All site accesses will be monitored and recorded.

- Filtering software will be used to prevent access to some sites that are clearly not work related or may have illegal content. Filtering software will be used to block, as far as possible, access to sites that involve extremist organisations and/or promote beliefs contrary to British values.

- A physical firewall will be installed and maintained to ensure that unauthorised external access to the network is prevented.

Wireless Infrastructure

- A wireless network is provided for direct access to the College's network and internet for all authorised devices.
  - Wifi access points (AP) will be monitored to ensure that an adequate service is provided to all users.
  - Security systems will be maintained to try to ensure, where possible, that the facilities are not misused'
  - Users will use their College Account to access to the wireless network.
  - Wireless communications between AP and client will be encrypted.

Remotely Accessible College Systems

- Processes will be implemented to protect college systems when accessed from outside the college by either college network users or third parties.
  - College web-based systems such as ProPortal will be made available through appropriate single sign on technologies such as LDAP or Azure authentication.
  - Where appropriate and in line with best practice and national guidelines multi-factor authentication (MFA) will be applied
  - Where appropriate dedicated access by approved IP will be implemented
  - Firewall systems will be configured to only allow authorised traffic onto the network.
  - Third Party Access has to be pre-authorised and reviewed by the IT Infrastructure and Technical Manager and/or Executive Finance Director with reference to the documented procedures in line with business case requirements.

E-Mail

- Access to the e-mail service will be granted using the same procedure as for access to systems and services.

- E-mail will only be used for college related purposes in line with the College IT Acceptable Use Policy

- Email filtering controls, e.g., anti-malware, spam, etc. will be implemented using Office 365 systems.

- Guidance on recognising phishing and related emails will be given which may include targeting users with phishing test emails to identify users who require further training.

- The use of e-mail will be monitored to protect against inappropriate use of the service.

Printing and Copying

- Where appropriate print and copy usage records will be maintained to measure quality of performance.

- All printing and photocopying is logged against budget cost centres. Monitoring takes place on a monthly basis and printing and photocopying costs are recharged to the relevant department via the Finance Department.

- All printer consumables, will be ordered and managed through the central admin team.

5. Physical Security

- All equipment will be used in accordance with the College Health & Safety policy.

- For ICT suites and rooms:
  - risk assessments will be undertaken, and appropriate physical security arrangements put in place.
  - the rooms will be locked, and windows closed when not in use.
  - the rooms will be kept clean and tidy and combustible and other waste removed each day.
  - eating and drinking, including chewing gum and eating sweets, will not be allowed in the rooms.
  - All computers will be logged off when not in use and shutdown if they are not to be used again on the same day.

- For equipment located in other areas:
  - based on perceived risk and value, equipment located in public areas may be 'locked down' or secured.
  - all computers should be logged off when not in use and shutdown if they are not to be used again on the same day.

- The moving of equipment and the installation of cables will only be carried out on the authority of the IT Department.

- For network cabling:
  - Cabling will, wherever possible, be housed in high quality trunking and hidden in ceiling voids.
  - Loopback protection and other security measures will be included on network switches.

Use of IT Facilities within Classrooms

- Equipment will be used appropriately with consideration for health and safety implications and the security of the equipment
  - All classrooms, where appropriate will have IT projectors or LCD screens, linked to a computer with ceiling/wall mounted amplified speakers.
  - The projectors will be installed in such a way as to minimise the chances of staff or students looking into the beam of the projector, e.g., by ceiling mounting or using 'short- throw' projectors mounted above the board.
  - Electronic whiteboard software will be installed and maintained by the IT Department.

6. Disposal of ICT equipment, recording media and college data

- The College will ensure through the IT Department that;
  - All obsolete or damaged ICT equipment and recording media will be disposed of in a secure manner;
  - Disposal of data in paper or electronic form complies with legislation and best practice;
  - Disposal & data erasing to be conducted through the use of an approved WEEE IT Recycling company and in accordance with the requirements of the GDPR and other legislative / statutory requirements including the Hazardous Waste Act and WEEE Directives 2005.

7. Data Backup & Restore

- A data back-up and restore procedure will be implemented with disaster recovery/business continuity (i.e., the ability to recover recent live data in the event of a partial or total loss of data) as the key deliverable.

- The back-up is not designed as a method of archiving material for extended periods of time.

- Backup Scope
  - The 'data' backups will at least cover all systems mentioned in the IT Disaster Recovery Plan.
  - All other systems will be included where the infrastructure resources allow. • At least 7 (daily) or 4 (weekly) restore points should be available onsite • At least one immutable full backup will be stored offsite.

- Data held and managed locally in departments is excluded unless departments have entered specific arrangements with IT.

- All staff are reminded that they are individually responsible for data held locally on their desktop or laptop computer and all critical data must be stored on the network drives. Student and staff network account data will be only restored from a duly authorised request.

- For key systems and services, data recovery and system restores will be tested regularly, as per IT Disaster Recovery Plan.

Appendix A: Associated Policies and Procedures

Associated policies:

- Data Protection Policy
- Document Retention Scheme
- ICT Acceptable Use Policy
- BYOD Policy
- Remotely Accessible IT Services
- IT Password Policy

Associated procedures:

- Starters and Leavers Process
- New Starter Form
- IT Disaster Recovery Plan
- System Update Procedure
- Firewall and Filtering-RFC-Procedure