BORDERS COLLEGE

Information Security Policy

November 2025

History of Changes

Version	Description of Change	Authored by	Date
1.1	Minor changes	F Wight	TBC – Glen Turnbull
1.2	Document overhauled. Additional information added around several areas including: • Incident management • Third-party access to systems • Procedure required for Cyber Resilience accreditation • Procedure required for GDPR compliance • Purchase, deployment and management of physical IT assets and college information assets	C Bradley	25/5/18
1.3	• Removal of references to British Standard Data Protection • Updated references to new college Data Protection policy • Removed references to use of games on systems as this is covered in 'Appropriate Usage of Electronic Systems' policy • Added references to DPIA where appropriate. • General housekeeping/ formatting • Clarified role of guidance and co-ordination around information security to come from Director of IT & Digital Head of ISLT • Removal of points around data classification • Update of references to Retention Schedule • DPO review	C Bradley	24/02/21
1.4	• Added information on Article 30 retention document and JISC retention guidelines in section 11. Change of role title for Head of ISLT to Director of IT & Digital	S Moncrieff	September 2023

2.0	• Formatting updates • Updated dept name from ISLT to IT & Digital • References to data protection removed as now covered in data protection policy • Updated guidance on usage of and storage of passwords and secrets • Information on IT Major Incident Procedure and Cyber Incident Response Procedure • Information on IT Disaster Recovery Plan • Added requirements around Identity and Access Management e.g. Multi-Factor Authentication (MFA) requirements • Added requirements for secure patching and configuration of systems • Added requirements for malware defence both for delivery and on devices	C Bradley	November 2025

Information Security Policy

1 Introduction

Information is a valuable resource. The College owns and uses vast amounts of information about its students, staff, suppliers and many other individuals and organisations. The College has a responsibility and a legal obligation to protect the information that it holds from loss or corruption and unauthorised access and modification.

This policy provides guidance on the College's information security requirements; identifies potential risks and highlights good practice. This policy is closely aligned with and should be read in conjunction with the Data Protection Policy.

2 Objectives

Provide management with direction and support in relation to information security in accordance with business requirements and relevant laws and regulations.

Promote sound information governance and facilitate effective resource management thus contributing positively to the College's vision and values.

Protect the College's information assets and IT services from all relevant threats.

3 Scope

This policy applies to all information assets, including verbal communications, hardcopy documents, data, software, storage media, web based and remotely hosted services, hardware and communications networks and the buildings within which such assets exist.

4 Responsibilities

The College will:

4.1 Protect its information from unauthorised access.

4.2 Assure confidentiality of sensitive information by protecting it against unauthorised disclosure.

4.3 Maintain integrity of information by protecting against unauthorised modification.

4.4 Assure availability of information in line with business requirements.

4.5 Meet regulatory and legislative requirements.

4.6 Produce, maintain and test business continuity plans to ensure that college services are able to be maintained as much as possible in the event of IT system failures while recovery takes place.

4.7 Ensure that all students, staff and other stakeholders are made appropriately aware of the information security policy.

4.8 Ensure that any breaches of information security, actual or suspected, are reported as soon as possible to the IT & Digital Learning team for investigation. Suspected breaches must be reported to the Helpdesk by visiting the IT helpdesk at the SBC campus in person, phoning 01896 662645 (externally) or ext. 2645 (internally). Reports may also be emailed to helpdesk@borderscollege.ac.uk but these reports must also be followed up with a phone call to ensure rapid response.

The following responsibilities for security are general in nature. Specific responsibilities are defined in the following chapters and by issuing role descriptions.

4.9 Each Vice Principal/Director is responsible for ensuring the security of information under their control in accordance with the advice provided by the Director of IT & Digital.

4.10 All managers are responsible for implementing this policy and any procedures referenced in this policy, within their areas of responsibility; for ensuring that their staff are properly trained and for adherence by their staff. Managers should consider how this policy integrates with their own operational procedures.

4.11 Every stakeholder and employee whether permanent, temporary or contract, has a responsibility when accessing College information to adhere to this policy and any procedures it references.

4.12 Any employee whose actions lead to a breach of policy will be liable to disciplinary action, up to and including dismissal, according to the College's disciplinary policy and procedures and/or legal prosecution.

4.13 Any Student whose actions lead to a breach of this policy will be liable to sanctions as per the College's Student Discipline Policy and Procedure and/or legal prosecution.

5 Organisation of Information Security

Specific Objectives:

Manage information security within the College.

Maintain the security of the College's information and information processing systems that are accessed, processed, communicated to, or managed by external parties.

Specific Responsibilities:

5.1 Vice Principals'/Directors' are responsible for the security of information under their control.

5.2 The Director of IT & Digital is responsible for the security and storage of data while it is held within the College's electronic infrastructure, or in web based/hosted systems and the management of all risks relating to that information.

5.3 The Director of IT & Digital is responsible for providing advice on information security and co-ordinating and communicating the guidance provided by in-house or specialist advisors throughout the organisation.

6 Asset Management

Specific Objectives:

Achieve and maintain appropriate protection of the College's IT & Digital assets. This covers:

- **Information assets** including digital data, paper documents, intellectual property, personally identifiable information, financial records, email and messaging content
- **Physical assets** including servers and storage devices, laptops, desktops, tablets, smartphones, network equipment (routers, switches, firewalls) portable media (USBs, external drives), printers, copiers, scanners, physical access cards, keys, security tokens
- **Software assets** including operating systems, business applications (CRM, ERP, HR systems), custom software and scripts, cloud-based SaaS applications, security tools (antivirus, SIEM, endpoint protection)
- **Cloud and virtual assets** including Cloud storage and databases, cloud-hosted applications, virtual machines and containers, APIs and integrations, identity and access management

Control the purchase (or acquirement in the case of free products/services) delivery, installation, location and disposal of all IT assets.

Ensure that information/data assets receive an appropriate level of protection.

Specific Responsibilities:

6.1 All major information assets will be accounted for and have a nominated owner.

6.2 Inventories of the important assets associated with each information system will be maintained.

6.3 With specific reference to the management of all manual records held by the College the Records Retention Schedule applies.

6.4 Devices are secured against malware either by prevention of its delivery or detection and response to stop their actions and quarantine the malware itself.

With specific reference to the management of IT Assets:

6.5 All College IT assets (including information/data assets) will be managed in line with the policies and procedures set out by the College.

6.6 All IT systems and services (inclusive of hardware with pre-installed software) required by the College must be purchased through the IT & Digital department.

6.7 The purchase of software, hardware or digital services by other departments through any other means, such as petty cash, credit cards or purchasing cards is strictly forbidden. This includes ‘free’ digital services due to the risks of personal data processing in unvetted systems.

6.8 Software, hardware and digital service acquisition channels are restricted to ensure a complete record of all purchases and that these can be registered, supported and upgraded accordingly. All newly purchased software, hardware and digital services must be delivered in accordance with the procedures agreed by the Director of IT & Digital.

6.9 All IT assets are processed through the IT & Digital asset procedure and the relevant IT & Digital asset register is updated.

6.10 Computer hardware may only be installed by the IT & Digital department. Exceptions are only allowed where clear, delegated authority is in place.

6.11 Under no circumstances should computer software (including shareware, freeware, public domain software and evaluation software) be installed by any employee, student or other individual on College equipment independently of the IT & Digital department except with the prior written consent of the IT & Digital department. This excludes cases where consent has been pre-approved such as apps available in the Company Portal app store on college issued devices.

6.12 External suppliers may install software under agreement with the IT & Digital department.

6.13 Electronic versions of software licences, invoices and installation software are backed up as part of the IT & Digital backup procedures.

6.14 The IT & Digital department must be notified in advance of all staff or department moves involving IT assets. Where required, an infrastructure check is conducted to identify necessary additions, removals and relocations of IT assets and the asset register is updated (as per the IT & Digital asset procedure).

6.15 Infrastructure checks and software and hardware movements are conducted by the IT & Digital department unless clear, delegated authority is in place.

6.16 The disposal of College software and hardware is carried out only by authorised members of the IT & Digital department.

6.17 Electronic and manual audits are conducted on a regular basis to ascertain the legality of all software identified. Sample random audits may also be carried out.

6.18 Where possible, all mobile computing equipment, e.g. laptops, mobile phones and digital cameras, are equipped with auditing software and are subject to periodic audit.

6.19 All College business data is backed up at a minimum daily to secure air-gapped immutable storage. Full details of the college's backup arrangements are not provided in this document for security but are available on request to approved staff and partners.

6.20 Malware delivery to devices will be reduced by:

- Filtering of web access
- Filtering of incoming email and attachments
- Blocking of USB drive access (unless approved for specific uses by IT & Digital)

6.21 All deployed end-user devices (other than those with managed app stores and restricted execution policy) will secured with Endpoint Detection & Response (EDR) software to detect and quarantine malware.

6.22 All servers will be secured with Endpoint Detection & Response (EDR) software to detect and quarantine malware.

6.23 All software deployed by the college will be kept up to date. All software on devices will:

- be licensed and supported
- removed from devices when it becomes unsupported or made safe by restricting to networks which have no access to college data
- have automatic updates enabled where possible
- be updated, including vulnerability fixes, within 14 days of release, where the update fixes vulnerabilities described by the vendor as 'critical' or 'high risk'

6.24 All devices deployed by the college will be configured in a secure manner. Configurations that result in vulnerabilities described by the vendor as 'critical' or 'high risk' will be patched within 14 days of identification.

7 Human Resources Security

Specific Objectives:

Reduce the risk of security breaches through theft, fraud, misuse of facilities or accidental acts.

Ensure that staff, third-party suppliers and partners and non-College employees with authorised access are aware of information security threats and concerns, their responsibilities and liabilities and are equipped to support organisational security policy in the course of their normal work.

Specific Responsibilities:

The College will ensure that:

7.1 All individuals with authorised access to College information and systems are made aware of their responsibilities for information security.

7.2 All individuals with authorised access to College information and systems are informed of specific responsibilities and given training where appropriate. This includes mandatory information security training for all college staff.

7.3 All potential employees are checked for suitability to the post in accordance with the College's Recruitment Process.

7.4 Where a current staff member's role changes significantly in relation to the information they are authorised to access and there is an increase of risk, suitability is checked in accordance with the College's Recruitment Process.

7.5 Employees and third-party suppliers are made aware of their legal responsibilities in relation to the confidentiality of the information to which they have access and must treat it appropriately. This includes non-transfer of confidential information to companies, individuals or data processing services that have not been approved for access to that data either through contract, approved and documented procedure or direct line-manager approval.

7.6 Employees and third-party suppliers are made aware of and fully understand, the proper channels for reporting security incidents, threats or weaknesses and software malfunctions.

7.7 Employees leaving college employment will have their access to college information assets and systems revoked at or before their final date of employment.

7.8 Third-party suppliers' access to college information assets and systems will be time restricted based on the period needed to complete their contracted work.

8 Physical and Environmental Security

Specific Objectives:

Prevent unauthorised physical access, damage and interference to the College's premises and information.

Prevent loss, damage, theft or compromise of assets and interruption to the College's business activities.

Specific Responsibilities:

8.1 Where sensitive information is processed there is a clear screen procedure.

8.2 A clear desk procedure is utilised as appropriate in areas where sensitive information is held and processed.

8.3 A clearly defined security perimeter surrounds areas containing secure information.

8.4 The force of the security perimeter is dependent on the type of information processed.

8.5 Access to areas where secure information is held and processed is restricted to authorised personnel and is monitored.

8.6 Effective controls exist in areas where secure information is processed, to ensure monitoring of all access.

8.7 There are effective controls for securely handling information assets away from secure areas.

8.8 Where possible, the location of secure information is kept confidential.

8.9 Secure information is protected from environmental hazards e.g. fire or flood.

8.10 Where identification badges are provided, they must be displayed during access to college buildings.

8.11 Equipment is sited or protected to reduce the risk of damage, interference and unauthorised access.

8.12 Equipment and media are removed from college premises only if authorised by college managers.

8.13 Users of mobile computing facilities, or users of any electronic equipment capable of storing data away from college premises, are responsible for the physical security of the devices being used and for ensuring that use of all electronic equipment complies with relevant information policies.

8.14 Network points in public areas are physically and electronically protected to reduce the risk of unauthorised access.

9 Operations Management

Specific Objectives:

Ensure the correct and secure operation of IT services, systems and end-user devices.

Specific Responsibilities:

9.1 Formally documented operational procedures for all of the College's IT systems, networks and media are established, maintained and securely stored.

9.2 All changes to facilities and systems are subject to change control procedures and must be assessed and authorised at the appropriate level.

9.3 Where practical, duties are segregated to reduce the risk of unauthorised modification or misuse of information or services.

9.4 Monitoring and audit trails are implemented.

With specific reference to the management of systems:

9.5 Development and operational software are run on different processors or in different domains or directories.

9.6 Development and testing activities are separated as far as possible.

9.7 Compilers, editors and other system utilities are not accessible from production systems when not required.

9.8 Different log-on procedures are used for production and test systems to reduce the risk of error. Different passwords should be used for these systems.

9.9 Development staff only have access to production passwords for the support of production systems. Controls are in place for issuing of the passwords and changing them after use.

9.10 Potential risks from external facilities management must be identified in advance and appropriate controls agreed and incorporated into the contract.

9.11 Capacity demands are monitored and future demands projected to ensure adequate processing power and storage are identified and managed.

9.12 Acceptance criteria for new systems or upgrades are documented and suitable tests carried out prior to acceptance.

9.13 Back-up copies of essential business information are taken regularly and an appropriate number of cycles kept, depending on the application.

9.14 Back-up copies and documented restoration procedures are stored securely at a remote location at a sufficient distance to escape any damage from a disaster at any of the main sites.

9.15 Restoration procedures are tested regularly to ensure that they are effective.

9.16 All of the College's wide and local area data provision is managed by the IT & Digital department unless clear delegated authority is in place.

9.17 Connection to the corporate data network is permitted only with the prior approval of the Director of IT & Digital or a delegated IT Manager.

9.18 Premises connected to the corporate network are assessed for risk. Appropriate measures are taken for high-risk premises.

9.19 Data networks are managed in such a way as to prevent unauthorised logical and physical connection and to detect unauthorised connection should this occur.

9.20 Subject to overall cost considerations, the data networks are designed and configured to minimise damage caused by any single component or link failure.

With specific reference to the management of data:

9.21 All media and sensitive documentation is protected from damage, theft and unauthorised access.

9.22 All confidential or sensitive data must be erased prior to the disposal of redundant media.

9.23 Media that cannot be erased must be destroyed physically by the College or by a third party under a contracted agreement.

9.24 The physical or electronic exchange of any software and/or data between the College and external parties is subject to formal agreement or contract. Appropriate compliance with legislation and standards shall be applied.

9.25 All storage, processing or transmission of payment cardholder data must be compliant with the latest version of the Payment Card Industry Data Security Standard (PCI DSS).

9.26 Where practicable, sensitive or confidential data is encrypted before transmission across Electronic Data Interchange (EDI) links.

9.27 Where practicable, EDI applications include precautions to deal with the possibility that data has been intercepted or modified during transmission and include checks that data has been dispatched and delivered in accordance with the system requirements.

9.28 Where appropriate, digital certificates or two factor authentication tokens will be used to authenticate the identity of the sender.

9.29 Physical media is suitably protected from unauthorised access, misuse, loss, damage or corruption while in transit.

9.30 Electronically published information, whether internet or intranet is protected from unauthorised modification.

9.31 Information will be made available in line with current information laws including that relating to Data Protection, Freedom of Information, Environmental Information Regulations, Re-use of Public Sector Information Regulations, Privacy and Electronic Communications Regulations, Public Records Act and Copyright.

10 Identity and Access Management

Specific Objectives:

Control access to the College's information and information systems.

Ensure authorised user access and prevent unauthorised access, compromise or theft of the College's information and information processing systems.

Specific Responsibilities:

10.1 Access is only granted to information and systems that are essential for individuals to carry out their duties.

10.1 Access is only granted to information and systems that are essential for individuals to carry out their duties.

10.2 Access is authorised by the manager responsible for the dataset.

10.3 Access is granted, maintained, revoked and monitored in a manner that avoids any conflict of interest between those granting the access and the people requiring access to the systems.

10.4 All access rights are reviewed at a frequency consistent with the business risks.

10.5 Special controls apply to the use of privileged access facilities such as those for systems administrators.

10.6 Connection of third-party suppliers and partners is subject to risk assessment.

10.7 Appropriately configured gateways and firewalls protect connections between the College's wide area network and external networks.

10.8 Access control lists and appropriately configured communications devices are used to control access in the internal network.

10.9 Users of mobile computing facilities, or any computer equipment away from college premises, must ensure that unauthorised persons do not overlook, or have access to, the information being accessed.

10.10 Remote users are authenticated prior to being granted access.

10.11 Repeated, unsuccessful logon attempts shall lead to denial of service and subsequent investigation. A notable exception is the un-locking facility provided by password self-service facility.

10.12 Connection to systems is timed-out after a period of inactivity, dependent on the criticality of the system.

10.13 Diagnostic ports are securely controlled.

10.14 Users are initially issued new passwords by a secure method. These will change immediately if the application allows user change of password.

10.15 Passwords are selected in accordance with the Password Management Policy.

10.16 Password users ensure that their passwords remain confidential.

10.17 Any use of group passwords must be based on a detailed risk assessment and approved by the Director of IT & Digital.

10.18 Unattended equipment is logged off or protected by a screensaver password.

10.19 Transaction accountability is maintained.

10.20 Logs of critical system activity shall be maintained for subsequent independent review.

10.21 Managers are responsible for ensuring that the access rights of their staff are consistent with requirements.

10.22 Techniques such as redaction, anonymisation and aggregation of data will be utilised as required to prevent unauthorised access to personal information.

10.23 Encryption, or other cryptographic controls, should be used where the College considers the information involved to need such security.

10.24 Administrator or super user level access to business-critical systems will be restricted to IT & Digital staff only for standard operations. IT & Digital will operate specific onboarding and access procedures for its staff to control accounts with this level of access.

10.25 Administrator or super user level access to business-critical systems may only be extended to staff outside of IT & Digital on a time-limited basis after the completion of a relevant risk assessment and approval by the Director of IT & Digital.

10.26 All college services are set to lock accounts after a maximum of 10 unsuccessful login attempts or limit the number of login attempts to no more than ten within five minutes to defend against brute-force attacks.

10.27 All college services mandate a minimum account password length of 8 characters with MFA or 12 characters in the absence of MFA. Longer and more complex passwords are supported and encouraged in our Password Guidance document.

10.28 All services exposed to the internet will be secured with MFA.

10.29 The college supports and encourages the move to ‘passwordless’ authentication such as FIDO2 keys and Passkeys wherever possible, especially for admin level accounts.

10.30 Account login details including passwords may never be stored unencrypted on college systems.

10.31 Service ‘secrets’ such as cryptographic keys or app secrets may never be stored unencrypted on college systems.

10.32 Account login details and service ‘secrets’ must not be transferred in cleartext e.g. emails/unencrypted shared files.

10.33 Accounts for college systems will be regularly audited, either by automation or where this is not possible by manual review.

11 Information Systems Acquisition, Development and Maintenance

Specific Objectives:

Ensure that security is an integral part of information systems.

Prevent errors, loss, unauthorised modification or misuse of information in applications.

Ensure the security of system files, application system software and information.

Specific Responsibilities for the IT & Digital department:

11.1 Business requirements for new systems, or enhancements to existing systems, must specify the requirements for security controls.

11.2 All new contracts for externally hosted systems must meet the College's information security standards and requirements and comply with relevant legislation including Data Protection, Freedom of Information, Environmental Information Regulations, Privacy and Electronic Communications Regulations, Public Records Act and Copyright.

11.3 Security controls reflect the business value of the information assets involved and the potential business damage from failure or absence of security.

11.4 Formally documented systems development, maintenance and testing procedures are established, maintained and stored securely.

11.5 Input data is validated to ensure it is correct and appropriate.

11.6 Systems incorporate validation controls to protect the integrity of data from processing errors or deliberate acts.

11.7 Output data is validated to ensure that it is correct and appropriate.

11.8 Cryptographic controls, such as encryption, digital signatures and non-repudiation services, are used where the College considers the information asset to need such security.

11.9 Only staff with appropriate IT authorisation may update production software.

11.10 Evidence of successful testing and user acceptance is needed before executable code becomes operational.

11.11 System test data is protected and controlled.

11.12 Operational data containing personal information is not used for testing purposes, unless de-personalised before use.

11.13 Program source libraries and production software is strictly controlled and accessed only by authorised staff.

11.14 Copying and maintaining program source libraries and production software is subject to Change Control procedures.

11.15 Periodic checks are made to ensure that no unauthorised changes have been made to live software.

11.16 Program listings and copies of third-party software are held in a secure environment.

11.17 Software packages are purchased only from reputable suppliers.

12 Incident Management

Specific Objectives:

Ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

Ensure a consistent and effective approach is applied to the management of information security incidents.

Specific Responsibilities:

12.1 All employees and third-party partners and suppliers have a responsibility to report any observed or suspected security weakness in College information systems as described in point 4.8

12.2 All information security incidents must be reported as described in point 4.8

12.3 Where third parties are holding information on behalf of the College they have a contractual and legal duty to report all incidents which may impact on the safety and security of College data as described in point 4.8.

12.4 The IT & Digital team will maintain an IT Major Incident Procedure and Cyber Incident Response Procedure that will lay out the IT & Digital team response in the event of an incident that is a threat to information security, whether through accident, negligence or malicious cyber-attack. The procedures will cover

- The declaration of IT Major Incidents/Cyber Response
- Formation of an IT Major Incident team
- Communication of incidents to the exec team (including where this then triggers the college's overall Business Continuity Plan)
- Communication of incidents to IT service users
- Technical responses to incidents including contact with external bodies and support partners
- Recording of incidents
- Review of incidents to investigate root cause and actions arising
- Closure of incidents

12.5 The IT & Digital team will also maintain an IT Disaster Recovery Plan to assist in the recovery of IT systems and services during or after an IT Major Incident or Cyber Incident covering:

- Preparation in advance of an IT Disaster to assist with recovery
- Responsibilities
- Communication
- Service restoration
- Plan maintenance and testing

13 Compliance

Specific Objectives:

Avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.

Ensure compliance of systems with organisational security policies and standards.

Maximise the effectiveness of and to minimise interference to/from the system audit process.

Specific Responsibilities:

13.1 All relevant statutory, regulatory and contractual requirements are defined explicitly and documented for each information system.

13.2 Appropriate procedures are implemented to ensure compliance with legal restrictions on the use of material in respect of intellectual property rights and on the use of proprietary software products.

13.3 Important records of the College are protected from loss, destruction and falsification.

13.4 Controls are applied to protect personal information in accordance with college policy and relevant legislation.

13.5 Management shall authorise the use of information processing facilities and ensure controls are applied to prevent the misuse of such facilities.

13.6 Controls are in place to enable compliance with national agreements, laws, regulations or other instruments to control the access to or use of cryptographic controls.

13.7 Where action against a person or organisation involves the law, either civil or criminal, the evidence presented conforms to the rules for evidence laid down in the relevant law or in the rules of the specific court in which the case will be heard. This shall include compliance with any published standard or code of practice for the production of admissible evidence.

13.8 Information systems are regularly checked for compliance with security implementation standards.

13.9 System audit controls of operational systems are carefully planned and agreed to ensure the minimal risk of disruption to business processes.

13.10 Access to system audit tools is protected to prevent any possible misuse or compromise.

13.11 Managers shall regularly undertake audits of the security procedures within their area of responsibility and take appropriate action to ensure full compliance with security policies and standards.

14 Related Procedural Documents

- Electronic Systems Policy and Procedure
- Social Media Policy and Guidelines
- Data Protection Policy and Data Protection Impact Assessment (DPIA) procedure
- Password Guidance document
- IT Disaster Recovery Plan
- IT Major Incident Procedure
- Cyber Incident Response Procedure
- Disciplinary Policy and Procedures
- Whistle Blowing Policy

15 Review

This Policy will be reviewed every 2 years or more regularly as circumstances dictate.

Status:	Approved
Policy Dated:	November 2025
Author:	Director of IT & Digital
Review Date:	November 2027
Equality Impact Assessed:	Yes