BORDERS COLLEGE

Working Together

Information Security Policy

May 2018

History of Changes

Version	Description of Change	Authored by	Date
1.1	?	F Wight	?
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

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. It is fully supported by a range of College policies and procedures.

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 from all relevant threats.

Ensure our information security meets our obligations under the Data Protection legislation; the Scottish Information Sharing Toolkit (SIST); and facilitates data sharing between the College and all of our partner organisations, at both a local and a national level.

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 information and vital services are available to users when they need them.

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

4.8 Ensure that all employee breaches of information security, actual or suspected, are reported quickly to the relevant line manager and investigated appropriately. All breaches must be reported to the Helpdesk by phoning 2645 or emailing helpdesk@borderscollege.ac.uk

4.9 Ensure that all stakeholder breaches of information security, actual or suspected, are reported to the Principal and investigated appropriately. All breaches must be reported to the IT Helpdesk by phoning 2645 or emailing helpdesk@borderscollege.ac.uk

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

4.11 Each Vice Principal/Director is responsible for ensuring the security of information under their control in accordance with the advice provided by the Vice Principal - Finance and Resources.

4.12 The Digital Development Group is responsible for ensuring that the policy is maintained and reviewed at least annually and for providing advice and guidance on implementation. Supporting policies will be authorised by standard college approval procedure.

4.13 All managers are directly responsible for implementing the policies, procedures and guidelines within their areas of responsibility; for ensuring that their staff are properly trained and for adherence by their staff. Managers should consider and where appropriate integrate, information governance aspects such as security, data collection and handling, within their operational procedures.

4.14 Senior Leadership Team members should ensure that regular random checks are carried out to confirm that personal data held remains relevant and is not retained for longer than necessary.

4.15 Every stakeholder and employee whether permanent, temporary or contract, has a responsibility when accessing College information to adhere to relevant policies, procedures and guidelines.

4.16 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.

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

4.18 Third-party partners and suppliers and authorised non College employees are subject to a documented risk assessment prior to gaining access to the College's information assets and are required to adhere to the College's policies and procedures. The ISLT department will hold a register of all documented risk assessments.

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, including corporate responsibility for data sets where the Data Manager is employed by their department and for ensuring that information security is actively considered in any review of their procedures.

5.2 The Digital Development Group is responsible for ensuring that the policy is maintained and reviewed at least annually and for providing advice and guidance on the production of supporting procedures and guidelines and their implementation.

5.3 The Head of ISLT 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.

5.4 The Director of Business Improvement and Performance 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.

5.5 Data Managers are responsible for maintaining the data quality of the data sets within their remit; for controlling access to them and for ensuring that the data sets are correctly identified in the College's Information Asset Register.

5.6 New information processing facilities are subject to a formal management authorisation process that will include checking that all security policies and requirements are met. This includes a Data Protection Impact Assessment which will be reviewed by the college Data Protection Officer.

6. Asset Management

Specific Objectives:

Achieve and maintain appropriate protection of the College's assets.

Control the purchase, delivery, installation, location and disposal of all IT assets.

Ensure that information receives 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 Information assets will be classified to indicate the level of sensitivity and business criticality.

6.4 Classifications will be reviewed regularly.

6.5 Information assets will be labelled and handled in accordance with the classification.

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

With specific reference to the management of IT Assets:

6.7 All College IT assets will be managed in line with the policies and procedures set out by the College.

6.8 All IT systems (inclusive of hardware with pre-installed software) required by the College must be purchased through the ISLT department.

6.9 The purchase of software and hardware by other departments through any other means, such as petty cash, credit cards or purchasing cards is strictly forbidden.

6.10 Software and hardware acquisition channels are restricted to ensure a complete record of all purchases and that these can be registered, supported and upgraded accordingly. Acquisition channels include internet sites.

6.11 All newly purchased software and hardware must be delivered in accordance with the procedures agreed by the Head of ISLT.

6.12 All IT assets are processed through the ISLT asset procedure and the relevant ISLT asset register is updated.

6.13 Computer hardware may only be installed by the ISLT department. Exceptions are only allowed where clear, delegated authority is in place.

6.14 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 ISLT department except with the prior written consent of the ISLT department.

6.15 External software suppliers may install software under agreement with the ISLT department.

6.16 Physical software licences, invoices and original media for all software installed on College equipment is stored in fireproof storage facilities at locations nominated by the ISLT department where appropriate. Electronic versions of software licences, invoices and installation software are backed up as part of the ISLT backup procedures.

6.17 Where necessary and with clear, delegated authority, the original media may reside with the user.

6.18 Software and hardware user manuals, if provided, will reside either with the user or with the ISLT department as appropriate.

6.19 The ISLT 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 ISLT asset procedure).

6.20 Infrastructure checks and software and hardware movements are conducted by the ISLT department unless clear, delegated authority is in place.

6.21 The disposal of College software and hardware is carried out only by authorised members of the ISLT department.

6.22 The use of games or screensavers, other than games that form part of the operating system or the standard screensaver, is not permitted except in special cases where authorisation has been granted by the Head of ISLT or a delegated officer.

6.23 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.

6.24 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.

6.25 All College business data is backed-up every 24 hours to disk with extended retention to tape. Business critical data is also replicated to a secondary data centre. Tapes will be kept in a fireproof safe at a secure College off-site location. The College does not back-up local PC drives.

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.

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.

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 policy 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 Management.

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 protected to reduce the risk of unauthorised access.

9. Communications and Operations Management

Specific Objectives:

Ensure the correct and secure operation of information processing facilities.

Specific Responsibilities:

9.1 Formally documented operational procedures for all of the College's computer 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 Incident management procedures are produced and maintained to ensure quick effective response to faults and failures of information processing systems and communications networks and any security breaches.

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

9.5 Monitoring and audit trails are implemented.

With specific reference to the management of systems:

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

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

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

9.9 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.

9.10 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.

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

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

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

9.14 Precautions are taken to detect and to prevent the introduction of malicious software e.g. viruses, worms, Trojan horses.

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

9.17 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.

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

9.19 All of the College's wide and local area data and voice communications equipment and all wireless provision is managed by the ISLT department unless clear delegated authority is in place.

9.20 Connection to the corporate data network is permitted only with the prior approval of the Head of ISLT or a delegated IT Manager.

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

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

9.23 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:

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

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

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

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

9.28 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).

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

9.30 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.

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

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

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

9.34 Information will be made available in line with current legislation 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. Access Control

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.

10.2 Access is authorised by the Data Manager responsible for the data set.

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 Head of ISLT.

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 Where the College's protective marking scheme is in use documents are appropriately marked in accordance with the scheme.

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

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

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

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

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 ISLT department:

11.1 Business requirements for new systems, or enhancements to existing systems, 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 Cryptographic keys are managed to protect against modification, destruction and unauthorised disclosure.

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

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

11.12 System test data is protected and controlled.

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

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

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

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

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

11.18 Software packages are purchased only from reputable suppliers.

11.19 Standards are set for third-party software to cover licensing arrangements, intellectual property rights, escrow agreements, supplier access rights and quality of code.

12. Information Security 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.

12.2 All information security incidents must be reported to the relevant line manager and logged with the IT Helpdesk. Incidents which are identified out-with normal working hours should be notified at the earliest possible opportunity.

12.3 All information security incidents, including those involving electronic data, paper files, images, verbal recordings, equipment and communication networks, logged with the IT Helpdesk, will be monitored and reported on regularly to the Senior Leadership Team.

12.4 Where third parties are holding information on behalf of the College they have a duty to report all incidents which may impact on the safety and security of College data.

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. Further information is provided in the Records Management Schedule.

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

- European General Data Protection Policy
- Data Protection Act 1998
- Disciplinary Policy and Procedures
- Whistle Blowing Policy
- Freedom of Information
- Electronic Systems Policy and Procedure
- ICT Change Management Policy
- Use of Laptop Procedure
- E-mail and Internet Policy and Procedure
- Social Media Policy and Guidelines

15. Review

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

Equality Impact Assessment

(Rapid impact assessment tool)

What Impacts may there be from this proposal on any group's ability to use the College services?

Policy: Information Security Policy

Positive Impacts (Groups affected)	**Negative Impacts (Groups affected)**
N/A	No groups have been identified where this policy is expected to have a negative impact.
Actions taken to alleviate any negative Impacts: N/A	
Recommendations: N/A	

From the outcome of the rapid equality impact assessment, have negative impacts been identified for any protected characteristic or any other potentially disadvantaged group?

No

Has a full Equality Impact Assessment been recommended?

Yes ☐

No x

Reason for recommendation:

Status:	Approved
Policy Dated:	September 2018
Author:	Interim ISLT Manager
Review Date:	September 2020
Equality Impact Assessed:	Yes