Information Security Policy

Written by: Richard Brine
CLT Sponsor: Steve Campion
Consulted with: SLT
Next Review Date: August 2020
Version: August 2018

Contents

1. Purpose

1.1. Exeter College collects and processes large volumes of information. In addition to discharging its obligations to protect data belonging to individuals, the college recognises that maintaining the integrity and security of personal, commercial and intellectual information is critical to its continued success.

1.2. The purpose of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or operated by Exeter College and to ensure compliance with legislation where that is relevant. This will be achieved through:

- Vigilance in respect of cyber crime and related threats
- Protecting information assets under the control of the organisation
- Describing the principles of security and ensuring that all members of staff fully understand their own responsibilities
- Embedding a consistent approach to information security as an integral part of day to day business
- Ensuring that members of staff are aware of, and fully comply with, relevant legislation

1.3. The policy aims to ensure that:

- Access to data and information systems is confined to those with appropriate authority in order to preserve commercial and personal confidentiality
- The ability to append, amend and delete data is subject to appropriate controls in order to preserve the quality and integrity of information
- Information is available to authorised personnel when and where it is needed
- An appropriate response is made when information assets are compromised

1.4. This policy applies to all information, information systems, networks, applications, locations and users of Exeter College or supplied under contract to it.

2. Definitions

2.1.1. **Cloud-hosted systems** are systems and data-sets which are not operated from or stored on hardware and premises owned by the college.

2.1.2. **Eduroam** is the secure, world-wide roaming access service developed for the international research and education community

2.1.3. **FFM** is the department for Finance, Funding and MIS

2.1.4. **ILS** is the department for Information and Learning Services

2.1.5. **Ja.net** is the UK higher, further education and skills sectors' not-for-profit organisation for digital services and solutions. Ja.net provides the internet service to the college.

2.1.6. **Penetration testing** is specialist testing to determine the ease with which a malicious attacker could gain unauthorised access to college systems and the potential impact this may have.

2.1.7. PaaS (Platform as a Service) is a class of Cloud-hosted services providing server capacity at Operating System level into which clients install and manage applications of their choice.

2.1.8. SaaS (Software as a Service) is a class of Cloud-hosted services providing fully managed software applications direct to the user.

2.1.9. SDG is the Systems Development Group

2.1.10. WEEE regulations are the Waste Electrical and Electronic Equipment Regulations 2013 which impose obligations on manufacturers and users in respect of the decommissioning, recycling and disposal of electrical and electronic equipment at the end of its useful life.

3. Policy

3.1. Responsibilities for information security

3.1.1. The Senior Leadership Team (SLT) member responsible for oversight of this policy is the Vice Principal (Finance and Business Operations).

3.1.2. Responsibility for the authoring, maintenance and operation of the policy rests with the Head of Information and Learning Services. The Head of ILS is responsible for monitoring, documenting and communicating information security requirements throughout the organisation.

3.1.3. The Systems Development Group sets standards which inform technical strategies to be implemented by teams in FFM and ILS.

3.1.4. The Heads of FFM and ILS are accountable for the security of the systems in their control including maintaining adherence to the standards set by the Systems Development Group.

3.1.5. The Head of Information and Learning Services provides monthly reports on the operation of this policy to the Systems Development Group. Reports and strategies will be prepared for the Audit Committee and/or the Business Services Committee by the Head of ILS as requested

3.1.6. Heads of department and faculty are responsible for the standards of physical security and operational practices applied to information which is under their control and that of their staff.

3.1.7. All employees must comply with information security procedures in support of the maintenance of data confidentiality and data integrity.

3.1.8. Line managers are responsible for ensuring that every individual working under their supervision is aware of:

- The information security policies and practices applicable in their work areas
- Their personal responsibilities for information security
- How to access advice on information security matters
- The need and means to maintain vigilance against cyber crime and related threats

3.1.9. Each member of staff is responsible for the operational security of the information systems they use.

3.1.10. System users must not use their account to access college information systems for any purpose not directly associated with the discharge of their duties on behalf of the college.

3.1.11. Each system user must comply with the security requirements that are currently in force, and must work with due regard for the confidentiality, integrity and availability of the information to which they have access.

3.1.12. Where information is processed on behalf of the college by third-party organisations, a Data Processing Agreement must be in place before access is granted.

3.1.13. Where information is shared with third-party organisations, an appropriate agreement must be in place before any transfer takes place.

3.1.14. Where information is required to be shared with a government agency, the college will adhere to the information security arrangements provided by that agency in respect of the data transfer.

3.1.15. New systems and processes are designed to ensure privacy by default.

3.1.16. Privacy Impact Assessments are conducted when required by legislation.

3.2. **Technical policy**

3.2.1. The architecture of college ICT systems will be devised to balance functionality, cost and security risk as directed by the Senior Leadership Team and the Systems Development Group as appropriate.

3.2.2. Network, server and storage environments will be configured according to manufacturers' best practice and validated by third party review.

3.2.3. Proprietary line of business systems (HR, Finance etc.) will be configured according to manufacturers' best practice and with due regard to the risks inherent in the nature of the college's user-base. They may be subject to third-party security review within the internal audit regime.

3.2.4. Default and 'built-in' accounts must be disabled and their credentials changed prior to systems being brought into production.

3.2.5. Locally-built systems which interrogate or aggregate data from line of business systems will be appropriately designed, coded securely and subject to third-party security review within the internal audit regime.

3.2.6. Firmware, Operating Systems and Applications will be maintained at the optimum version / patch levels to balance reliability with security as agreed by the Systems Development Group.

3.2.7. Mechanisms for the remote administration of services will be secured using encrypted tunnel connections. Systems to be implemented 'in the Cloud' either as PaaS (platform as a service) or SaaS (software as a service) will be validated against security criteria agreed by the Systems Development Group.

3.2.8. Mechanisms for the transfer of data between local and Cloud-hosted systems will be validated against security criteria agreed by the Systems Development Group.

3.2.9. Consideration should be given to the need for encryption at the server of each dataset which comprises personal or other business-critical data. The recommendation to encrypt, or not, should be referred to the Systems Development Group and the resulting decision recorded in the register of datasets.

3.2.10. Regular, third-party, penetration tests will be commissioned in respect of internal and external threats across all college services. The outputs of such tests will be used by the Systems Development Group to inform approaches to secure systems-integration and development.

3.2.11. Logging and intrusion detection will be implemented to assist in the forensic investigation of inappropriate and criminal behaviour.

3.2.12. User access will be granted and withdrawn according to established procedure by the appropriate system administrator.

3.2.13. Employees' privileges over datasets will be assigned according to their job-role as documented by the appropriate systems administrator. Privileges will be limited to those records and attributes required for the effective discharge of each user's function within the college.

3.2.14. Technical measures will be maintained which prevent unauthorised equipment being connected to the college's networks.

3.2.15. Only users with an active Exeter College account (which may be a guest account) will be permitted access, external or internal, to the college's non-public facing services.

3.2.16. Where users are permitted to 'bring their own device', connection to college systems will be via the WiFi service and be subject to the standard controls at the perimeter of the internal network. Only those users with an active Eduroam or Exeter College account (which may be a guest account) will be permitted WiFi access to college and Ja.net services.

3.2.17. Users connecting their own devices to the college's mail and other services must agree to terms which include the remote erasure of college data from the device in the event that the college considers that such data may become compromised.

3.2.18. Personal data stored on mobile, removable and portable devices including USB flash drives and laptop computers must be encrypted to the standard agreed by the Systems Development Group.

3.2.19. College-owned mobile devices will be subject to Mobile Device Management systems which will enable tracking of such devices and the remote erasure of data from them.

4. Implementation

4.1. Management of security

4.1.1. Senior Leadership Team responsibility for information security resides with the Vice Principal (Finance and Business Operations).

4.1.2. Heads of department and faculty must ensure that the information processing procedures and practices, followed by them and their staff, meet the standards expressed in this policy.

4.2. Information security awareness training

4.2.1. Information security awareness training will be included in the staff induction process.

4.2.2. Information security guidance and resources will be made available via the Information Governance section of the Exeter College Portal.

4.2.3. An ongoing security and cyber crime awareness programme will be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

4.3. Contracts of employment

4.3.1. All contracts of employment will contain a confidentiality clause.

4.3.2. Information security expectations upon staff will be included within appropriate job descriptions.

4.4. Control of information assets

4.4.1. Each system or dataset, whether hosted locally or in the Cloud, will be managed by no less than two and no more than four named System Administrators.

4.4.2. The Head of the Department or Faculty in which the administrators are employed is accountable for the appropriate custodianship of that system or dataset.

4.4.3. Acting on behalf of the responsible Head, each System Administrator will ensure that access controls and privileges are granted and maintained to meet business and security needs.

4.4.4. The Register of Datasets will be maintained by the Head of Information and Learning Services detailing the volume and nature of each dataset, the names of its administrator(s), its location and security arrangements.

4.4.5. The sharing of personal data with data subjects and third parties is subject to the terms of the college's Data Protection policy and associated documents.

4.5. Systems administration standards

4.5.1. Employees whose role requires that they are granted extended administration privileges across one or more systems must work in accordance with the Code of Practice for Systems Administrators.

4.5.2. Wherever practical, system administration duties should be segregated from day to day operations. Where individuals are required to perform both operational and administrative duties, separate accounts should be used for each role and each account granted role-specific permissions.

4.5.3. Systems will be configured to provide the greatest possible level of auditing of administrative intervention.

4.5.4. Each System Administrator must adhere to standard auditable procedures which record the need, granting and withdrawal of permissions.

4.6. Access controls

4.6.1. Only authorised personnel who have a justified and approved business need will be given access to business systems or information storage locations.

4.6.2. Access to personal data will be limited to that needed by individual employees in order to discharge their job effectively and granted subject to the Data Protection Policy.

4.7. Computer Systems Access Control

4.7.1. Access to computer facilities will be restricted to authorised members of the college. Accounts will be granted only in accordance with standard procedures.

4.7.2. The standard(s) of authentication required for access to college systems will be determined by the Systems Development Group and informed by advice from the college's internal auditors.

4.7.3. The standard(s) of authentication required for access to business system applications must meet, at least, the standards applied to the Active Directory and will be held under review by the Systems Development Group.

4.7.4. The authentication standard presently in use is defined in section 6 of this policy.

4.8. Application access control

4.8.1. Access to data, system utilities and program source libraries will be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application will depend on the availability of a licence from the supplier.

4.9. Systems Integration

4.9.1. Data exchange and interoperability standards will be agreed, with due regard for information security, by the Systems Development Group.

4.9.2. Security considerations in respect of systems integration proposals will be reviewed by the Systems Development Group in light of any current or future recommendations from the college's internal or external auditors.

4.9.3. Systems integration should be designed to ensure privacy by default and privacy impact assessments carried out in compliance with current legislation.

4.10. Removable media

4.10.1. College datasets should not be copied onto removable media unless the transfer is supervised by the Head of FFM or Head of ILS. Smaller collections of personal or commercially sensitive data should only copied onto removable media with the permission of a Head of Department, Head of Faculty or SLT member. Permission should be granted only where there is no alternative secure means of transmission and where the data are protected by encryption.

4.11. Equipment security

4.11.1. In order to minimise potential loss or damage, all assets will be protected from physical threats and environmental hazards so far as is practical. Prior to deployment, ICT Services will security mark all removable ICT equipment using a code unique to Exeter College.

4.11.2. All redundant and unserviceable ICT equipment must be returned to ICT Services for secure data destruction and subsequent disposal according to WEEE regulations.

4.12. Protection from malicious software

4.12.1. The college will deploy software countermeasures and management procedures to protect itself against the threat of malicious software. Technical measures will be maintained to prevent the user-installation of software on the organisation's devices. ICT users breaching the 'Code of Practice for users of college ICT systems' may be subject to disciplinary action.

4.12.2. The college will employ security measures at the perimeter of the network in order to control external threats and internal-users' internet activity. ICT Services will control, record and review rule changes according to established procedure.

4.13. Computer and network procedures

4.13.1. Management of computers and networks will be controlled through standard documented procedures.

4.14. Information risk assessment

4.14.1. ICT Services will maintain a register of risks, including risks to information assets stored on its servers, together with planned control measures. The administrators of information assets stored elsewhere will be responsible for recording and managing risks to which those assets are exposed.

4.15. Information security events and weaknesses

4.15.1. The ICT Team will maintain and invoke a cyber-event response plan, approved by the College Business Continuity Group

4.15.2. All information security events will be investigated to establish their cause and impacts with a view to avoiding similar events.

4.15.3. The Head of ILS will maintain a protocol for the investigation and reporting of information security events.

4.15.4. The Head of ILS will report information security events to each meeting of the Systems Development Group.

4.16. Monitoring system access and use

4.16.1. In accordance with the Code of Practice for users of college systems, a log of system access and data-use by staff and students will be maintained.

4.16.2. In addition, the college reserves the right investigate activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000), together with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, permit monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime

- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system

4.16.3. The college may also process personal and communications data where this is necessary for the discharge of its statutory duties, for example duties in respect of the prevention of radicalisation.

4.16.4. Any monitoring will be undertaken in accordance with the above legislation and the Human Rights Act

4.17. Currency of information systems

4.17.1. The college will ensure that all information systems, applications and networks are maintained according to manufacturers' best practice. Workstation Operating Systems and applications will be maintained at the latest patch level according to established procedure and subject to testing where appropriate.

4.18. System change control

4.18.1. Changes to information systems, applications or networks will be subject to a formal change control process. All but minor changes will be reviewed and authorised according to established procedure. Significant changes will be agreed by the Systems Development Group and reported to the Systems Development Group.

4.19. Intellectual property rights

4.19.1. The college will ensure that all information products are properly licensed and approved by the Head of Information and Learning Services. Users will not install software on the college's property without permission from the Head of Information and Learning Services. ICT users breaching the Code of Practice may be subject to disciplinary action.

4.20. Business continuity and disaster recovery plans

4.20.1. The ICT Service will maintain a data backup regime, in respect of locally-hosted services, according to the needs of the college.

4.20.2. The ICT Service will be responsible for the recovery of mission-critical, locally-hosted, information, applications, systems and networks in the event of a disaster.

4.20.3. The administrators of Cloud-hosted services will be responsible for ensuring that appropriate back-up and recovery provision is in-place.

4.20.4. The administrators of non-ICT information systems will maintain recovery / business continuity plans for invocation in the event of a disaster.

4.21. Monitoring, review and evaluation

4.21.1. This policy will be reviewed in line with changes in legislation or good practice, or every two years, whichever is the sooner.

4.22. Further information

4.22.1. The effective implementation of this policy is dependent upon other components of the Information Governance framework and operating documents within the ICT Service and other college functions.

4.22.2. Related documents, information, advice and guidance on this policy can be obtained from the Information Governance section of the Portal or from the Head of Information and Learning Services.

5. Associated documentation

5.1. Code of Practice for Systems Administrators

5.2. Relevant Legislation

5.2.1. Exeter College is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation will be devolved to employees and agents of the college, who may be held personally accountable for any breaches of information security for which they may be held responsible. Exeter College will comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (2018)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Freedom of Information Act 2000
- Counter-Terrorism and Security Act 2015

6. User authentication standard

6.1. Active Directory Accounts (current at 11 March 2016)

6.1.1. User authentication is via username and password enforced throughout the Active Directory (AD) by means of Group Policy Operations to include:

- Password complexity (alphanumeric, upper and lower case, minimum 8 characters)
- Password lifetime (59 days, unique in 19 cycles)
- Lock out after 3 failed authentication attempts for a time period of 30 minutes

6.1.2. User-requests for password resets and other AD account changes will be managed by the ICT Service according to established procedure.

7. Equality Analysis

Please use the 'equality analysis procedure' to guide you to complete the text boxes below, expanding them as you wish. If this is a review - please add date and make any amendments if required.

Insert date reviewed

7.1. Is your policy equality- relevant? If yes, please list which groups of people will be affected by this policy. If no people are affected by this policy it has no equality relevance and you should write no and you need not answer any more questions.

Write here

7.2. How have you involved people from minority groups who may be affected by this policy? Describe any activities such as conversations, interviews, feedback or plans to do this in the future. *Write here*

7.3. What evidence have you considered? List any sources of data and research you have used. This can include college or national monitoring data, surveys, reports, consultations, focus groups, pilots, evaluations. Describe any ongoing data collection or plans for future research. *Write here*

7.4. How will your policy fulfil the public sector duty by helping fight discrimination, advance equality of opportunity and foster good relations?

Characteristic	How does your policy help fulfil the public sector duty? What Equality issues have you addressed?
Age	*Write here*
Disability	
Gender	
Pregnancy & maternity	
Race	
Religion and belief	
Sexual orientation	
Transgender	

7. 5. Describe any potential adverse impacts that may arise as a result of the policy. If any are identified, you should also state what actions will be taken to mitigate that negative impact. If yes, say if you have an action plan to carry this out? *Write here*