Information Governance Policy

Written by: Data Protection Officer
CLT Sponsor: Senior Information Risk Owner
Consulted with: ICT Manager, SIRO, ICO
Next Review Date: January 2024
Version: January 2022

1 Purpose and Scope

1.1 Exeter College collects and processes large volumes of information, which enable the College to deliver outstanding education and manage services and resources efficiently. Maintaining the integrity and security of this information, and ensuring its effective use for the intended purposes, is critical to the College's continued success. The Information Governance Policy aims to protect all resources which are crucial to the College.

1.2 This policy and its subsidiary policies aim to ensure that information stored and processed by or on behalf of Exeter College in any form (e.g. emails, voice messages, minutes, photographs, student records, staff records, financial records etc) or at any location, using any equipment (e.g. computers, laptops, tablets, mobile phones, cameras etc) is protected against breaches of confidentially, integrity or availability and the consequences of such breaches.

1.3 This policy applies to all information, information systems, networks, applications, locations and staff, students and contractors of Exeter College or associated third parties. Its main purpose is to help to manage information and to reduce risk to information assets to an acceptable level. This will be achieved through:

- A consistent approach to Information Governance as an integral part of day to day business
- Describing the principles around Information Governance and ensuring that all members of staff fully understand their own responsibilities
- Ensuring that members of staff are aware of and fully comply with this policy and its subsidiary policies

1.4 This policy sets aims to ensure the main Principles around Information Governance are implemented and maintained. Subsidiary policies and procedures are referenced to signpost further detail.

2 Definitions

2.1 **FFME** is the Department for Finance, Funding, MIS and Exams

2.2 **SIRO** is the College's Senior Information Risk Owner. The Exeter College's SIRO is the Chief Financial Officer (CFO). The SIRO is accountable for information risk across Exeter College and for sponsoring and promoting the Information Governance Policy.

2.3 **SLT** is the Senior Leadership Team, consisting of the Principal, Vice Principals and Assistant Principals of Exeter College.

2.4 **CLT** is the College Leadership Team, consisting of the SLT, Directors and all Heads of Business Support Departments and Teaching Faculties.

2.5 **IAO** is an Information Asset Owner. IAOs are accountable for ensuring their information assets are identified and compliant with all subsidiary policies and legislation.

2.6 **DPO** is the Data Protection Officer. The DPO and Compliance Manager is the DPO at Exeter College.

2.7 **SDG** is the College's Systems Development Group

2.9 **UK GDPR** are the General Data Protection Regulations

3 Policy

3.1 Accountability

3.1.1 The SIRO of Exeter College will oversee the Information Governance Policy program and delegate responsibility for information management to the IAOs, including the DPO and Compliance Manager, the ICT Manager and the College Leadership Team (CLT). The SIRO will be a senior executive and member of the Senior Leadership Team (SLT). The DPO will be the DPO and Compliance Manager.

3.1.2 All incidents around identified or suspected data breaches will be reported in line with Exeter College's Data Loss Response Procedure.

3.1 3 Exeter College will have an annual schedule of internal audits, based on the College's Risk Register and in line with its Risk Management Policy.

3.2 Transparency

3.2.1 Exeter College's business processes and activities, including its information governance program will be documented in an open, verifiable and understandable manner and documentation will be available to all staff at the College and relevant third parties.

3.2.2 Exeter College will inform students, staff and other stake holders of what information is collected about them and the purpose of processing. Collecting and sharing of personal data with data subjects and third parties will be subject to the terms of Exeter College's Data Protection Policy and associated documents.

3.2.3 Exeter College will ensure that all data subjects (students, staff and other stakeholders) know how to request access to their information, should they wish to do so.

3.3 Integrity

3.3.1 Exeter College will establish and maintain an information governance program to guarantee that information assets generated or managed by Exeter College staff have a reasonable guarantee of authenticity and reliability.

3.3.2 Exeter College will aim to ensure the integrity and authenticity of records in all media over time by

- providing training for all staff who interact with records and associated documentation
- using workflows to create audit trails where practicable
- maintaining reliable systems which control Exeter College's recordkeeping including hardware, network infrastructure and software

3.3.3 Exeter College will ensure correctness of and adherence to the policies and procedures maintained by the Corporation. All policies will be approved by the SLT and adopted by the Governors.

3.4 Protection

3.4.1 Exeter College's information governance program will ensure an appropriate level of protection to information assets that are private, confidential, privileged, secret, classified, essential to business continuity, or that otherwise require protection. To that aim, the College will maintain an Information Asset Register.

3.4.2 Exeter College will maintain a Business Continuity Plan in line with its Business Continuity Policy.

3.4.3 Exeter College will maintain a Risk Register in line with its Risk Management Policy.

3.4.4 Exeter College will conduct Data Privacy Impact Assessments (DPIA) where required. New systems and processes will be designed to ensure privacy by default, in line with the College's Data Protection Policy.

3.5 Compliance

3.5.1 The College's information governance program will comply with applicable laws, other binding authorities and other Exeter College policies.

3.5.2 Exeter College is obliged to abide by all relevant UK 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.

3.5.3 Exeter College is aiming to adopt a standards-based framework in accordance with its Information Security Policy and use the ISO 27001 specification with a view to possible accreditation. Exeter College has achieved and will maintain the Cyber Essential standard and is aiming to achieve Cyber Essential Plus.

3.5.4 Exeter College will comply with the following legislation and other legislation as appropriate:

- Data Protection Act 2018
- General Data Protection Regulations 2016
- Counter-Terrorism and Security Act 2015
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Freedom of Information Act 2000
- Data Protection (Processing of Sensitive Personal Data) Order 2000
- Human Rights Act 1998
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Health and Safety at Work Etc Act 1974

3.6 Availability

3.6.1 Exeter College will maintain its information and records in a way that ensures their timely, efficient and accurate retrieval to

- support all employees in their work
- ensure compliance for legal, audit and other regulatory review purposes
- validate management decisions
- account for resources

3.6.2 In line with its Information Security Policy the College will routinely back up electronic data so that it can be restored in case of disaster, malfunction or data corruption.

3.6.3 Exeter College will strive to regularly remove obsolete and redundant information from its systems to support effective management of its information assets.

3.7 Retention

3.7.1 Exeter College will maintain its information assets for an appropriate time, taking into account its legal, regulatory, fiscal, operational, and historical requirements.

3.7.2 Exeter College will maintain a Retention Schedule in line with its Retention and Disposition Policy.

3.8 Disposition

3.8.1 Exeter College will provide secure and appropriate disposition for information assets which are no longer required. The disposition of information will comply with applicable laws and the College's Retention and Disposition Policy.

4 Implementation

4.1 Roles and responsibilities

4.1.1 The Board of the Corporation and SLT agree and adopt the Information Governance Policy and subsidiary policies.

4.1.2 The SIRO is responsible for oversight of this policy. The SIRO will:

- be accountable to the Board regarding all relevant matters
- ensure that Exeter College's approach to information risk is effective and well executed
- support effective communication to staff
- ensure relevant resources and training are in place
- sign off the information asset register annually in July

- take ownership of the risk assessment process
- review and agree action in respect of identified information and cyber breaches
- approve all DSAR and FOI requests
- line manage the DPO
- sponsor and oversee the SDG

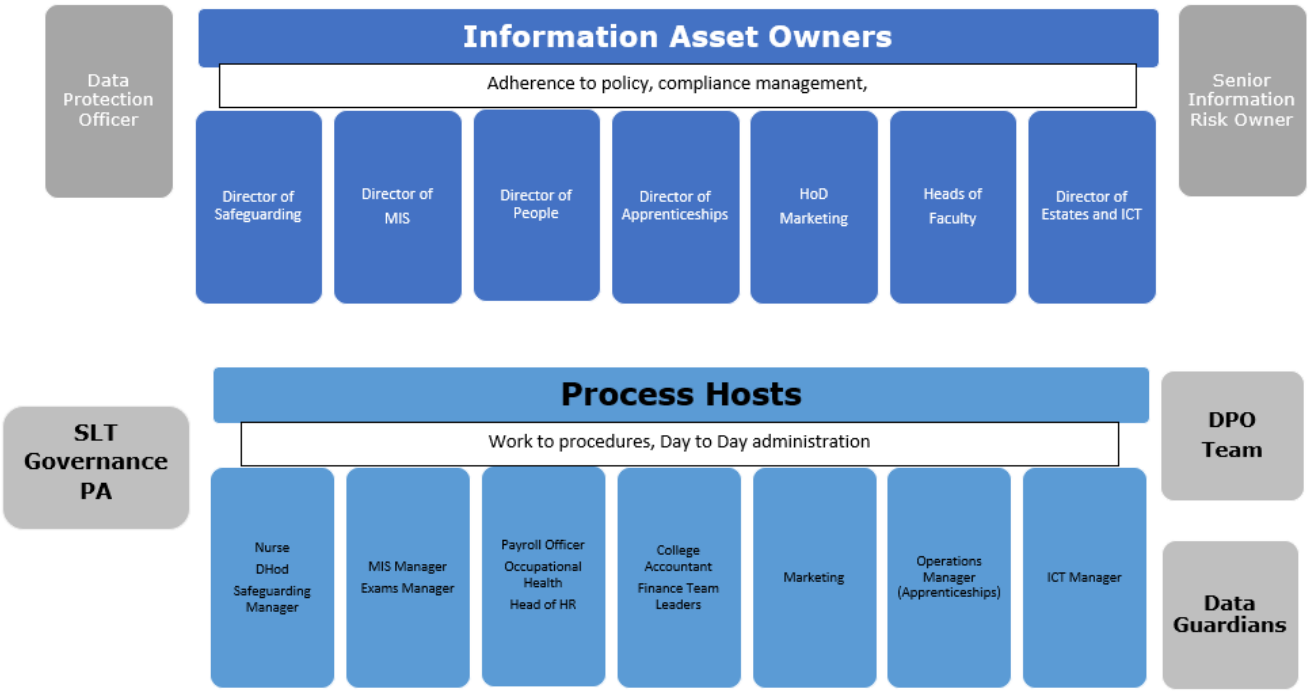
4.1.3 Responsibility for authoring, maintenance and operation of the policy lies with the DPO. The DPO will:

- be the contact for the ICO and individuals whose data is processed by Exeter College
- inform and advise Exeter College around its obligations relating to data protection legislation
- monitor Exeter College's compliance with information governance and data protection requirements
- review Data Protection Impact Assessments (DPIAs)
- develop and deliver relevant staff training to support information governance and data protection
- monitor Exeter College's policies and procedures
- support implementation of audit action plans
- monitor and support Freedom of Information requests and DSARs
- advise on and investigate identified information/data breaches
- advise and support Information Asset Owners
- be a core member of SDG

4.1.4 The ICT Manager will:

- ensure the security and compliance of IT systems at Exeter College
- report information and cyber security risks to the SIRO
- support and advise IAOs in relation to their information assets
- work with the DPO and Compliance Manager regarding data and IT security
- be a core member of SDG

4.1.5 Information Asset Owners (IAOs) are responsible for ensuring that specific information assets are handled and manged appropriately. They will ensure that information assets are properly protected and their value to the organisation will be fully exploited. The IAOs will be supported by the Process Hosts as set out below:



IAOs will

- support a culture that uses and protects information for the benefit of students, staff and other stakeholders
- ensure there is a legal basis for the processing of personal data and where relevant seek advice from the DPO

- support the DPO in monitoring and updating the Information Asset Register
- understand and monitor information flows to and from information assets
- inform the SIRO of any risks to the information assets

4.1.6 **The Systems Development Group** (SDG) will

- provide strategic direction and oversee strategic developments in relation to the College's systems development and IT provision
- understand the current IT and systems development requirements as well as new and future system developments across the Exeter College Group and its wider stakeholders
- ensure information security and data protection issues are considered as part of systems development and network/architecture design
- ensure that systems development is in line with, and makes a positive contribution to, the College's Strategic Plan
- ensure adequate training programs are in place across the college to reduce the impact of social hacking of College systems and increase awareness of information governance and data protection
- review and recommend for approval to SLT relevant policies and procedures

4.1.7 **The Heads of FFME and IT** are accountable for the security of the systems in their control, including maintaining adherence to the standards set by the SDG.

4.1.8 **Heads of Department and Faculty** are responsible for ensuring that the information processing procedures and practices followed by them and their staff meet the standards expressed in this policy and all associated policies and procedures. They will:

- Ensure Information Governance is implemented in their departments and faculties
- Encourage staff to report information and data breaches
- Work closely with the DPO and Compliance Manager and the ICT Manager to implement this policy and all subsidiary policies

4.1.9 **Line managers** are responsible for

- ensuring that every individual working under their supervision is aware of the policies associated with Information Governance and their personal responsibilities arising from adhering to associated procedures
- seeking advice and guidance from the DPO where needed

4.1.10 **All employees** will

- ensure they read the Information Governance Policy and subsidiary policies and seek advice where needed
- comply with procedures in support of this policy and subsidiary policies
- complete mandatory data protection training and attend at least one relevant information governance training session per academic year

4.1.11 **All students** will

- be made aware of procedures and protocols relevant to their communications with Exeter College staff and their peers
- be supported through their tutorial and the Personal Development Programme to develop their knowledge and understanding of cyber-Security and the UK GDPR
- be advised how to stay safe online and how to keep their own information and data safe

4.2 Training structure

4.2.1 Line managers are responsible to ensure their staff are aware of how to access support and guidance to enable them to comply with the Information Governance Policy and associated policies.

4.2.2 The DPO supported by the People Department, is responsible for providing training and to keep information and guidance up to date and relevant.

4.2.3 All staff must undertake mandatory training relating to Information Governance and Data Protection and attend relevant training sessions at least biannually to ensure that they are aware of and able to adhere to their responsibilities and legal obligations.

4.3 Contracts

4.3.1 All contracts of employment will contain a confidentiality clause.

4.3.2 Exeter College will implement Data Sharing Agreements with relevant third parties.

4.3.3 Third parties will abide by the Data Sharing Agreements.

4.4 Resources

4.4.1 Resource requirements to implement the Information Governance Policy and subsidiary policies will be provided by the SIRO and the SLT as appropriate.

5 Associated Documentation

5.1 **Policies** are available to all staff via the Exeter College Staff Hub and the Exeter College website

- Business Continuity Policy
- Data Protection Policy
- Information Security Policy
- Marketing Policy
- Retention and Disposition Policy
- Risk Management Policy
- Scope and Coverage Policy
- Whistleblowing Policy

5.2 **Procedures** are available to all staff via the Data Protection SharePoint

- Data Loss Response Procedure
- Data Retention Schedule
- Subject Access Request Procedure
- Identity Verification Procedure
- Police Disclosure Protocol

6 Monitoring, Review and Evaluation

6.1 The policy and any subsequent versions of it will be formally adopted on behalf of the College, subject to recommendations of the Senior Leadership Team, by the Board to the Corporation.

6.2 The DPO will oversee maintenance, review and monitoring of the Information Governance Policy.

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

6.4 The definitive version of this policy is stored on the College Leadership SharePoint page.