Glasgow Kelvin College

Information Security Framework

Document Control Information	
Reviewed by the SMT:	**November 2022**
Date of Next Review:	**December 2025**
Approved by Board of Management:	**12 December 2022**

The Board of Management (or any person/group with delegated authority from the Board) reserves the right to amend this document at any time should the need arise following consultation with employee representatives.

Table of Contents

1. Introduction

It is the policy of Glasgow Kelvin College that it will manage all its information appropriately and securely to protect against the consequences of non-compliance with data protection law, including breaches of confidentiality, failures of integrity or interruptions to the availability of that information.

This framework provides the structure for an interconnected set of College Information Security Policies and procedures. These aim to develop a positive culture of information security throughout the College through the development of a holistic Information Security Management System (ISMS) to protect College information by maintaining its confidentiality, integrity and availability.

- Confidentiality: a component of privacy that protects our data from unauthorised access or disclosure.
- Integrity: maintaining and assuring the accuracy and completeness of data over its entire lifecycle.
- Non-repudiation – the reasonable assurance that, where appropriate, a user cannot deny being the originator of a message after sending it.
- Availability: for any information system to serve its purpose, the information must be available when it is needed.

This framework aims to encourage the engagement and implementation by users of good information security practices throughout the College.

2. Objectives

The objectives of this framework are to:

- safeguard the College's information from both internal and external security threats that could have an adverse effect on its operations, financial position or reputation;
- fulfil the College's duty of care and legislative responsibilities in relation to the information with which it has been entrusted;
- protect the confidentiality, integrity and availability of information by ensuring adequate controls are in place so that information is appropriately available as required, is accurate, secure, and complies with legislative requirements;
- ensure that all users of the College's information understand their roles and responsibilities in relation to information security.

3. Scope

The scope of this Information Security Framework extends to all College information including but not limited to:

- Records related to prospective, current and past students and staff including emergency and next of kin contact information and special category data
- Records related to workers employed through third party agencies, members of the Board, visitors, customers, and external contractors

- Teaching and learning data
- Learner support data, including information about health and disabilities
- Financial records and information
- HR, including Occupational Health records, and Organisational Development data
- Health and Safety records
- Operational plans, account records and minutes
- Executive level data
- Student Association data
- Commercial and Business Development data
- Quality and Performance data
- Intellectual Property data
- External Funding records

4. Framework Statement

As a Data Controller, the College is accountable for the personal data it processes. This extends to its use of third parties acting as Processors on the College's behalf. It is the College's responsibility to ensure that they, and any Processors they use, comply with data protection law. Failure to do so, for example through the lack of appropriate due diligence, may result in the College facing regulatory action including fines.

Glasgow Kelvin College aims, as far as reasonably possible, to:

- Identify and protect the confidentiality, integrity and availability of all data (information assets) it holds within its systems by implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risk. This includes the protection of any device that can carry data or access data, as well as protecting physical paper copies of data.
- Take a data protection by design and default approach to any new data processing, including the use of new technology, to identify any risks by firstly carrying out a Data Protection Impact Assessment as required.
- Meet legislative and contractual obligations as required under the UK General Data Protection Regulation (GDPR), Data Protection Act 2018 and other relevant legislation.
- Protect the College's intellectual property rights.
- Produce, maintain and test business continuity plans particularly with respect to data backup and recovery.
- Prohibit unauthorised use of the College's information and systems.
- Communicate the requirements of this Information Security Framework and the information security aspect of procedures to all persons potentially accessing data as part of their role as appropriate.
- Provide information security training to all persons appropriate to their role.
- Report any breaches of information security, actual or suspected to the DPO in a timely manner noting that where a significant breach has occurred, the College must report this to the Information Commissioner's Office within 72 hours and data subjects may be notified.

5. Compliance

The College will conduct information security compliance and assurance activities, facilitated by the College's Digital Services, to ensure information security objectives and the requirements of the framework are met. Wilful failure to comply with the framework will be treated extremely seriously by the College and may result in disciplinary action and/or legal action.

6. Responsibilities

This framework covers all data access and processing within the College and through remote or mobile working.

All staff, Board Members, and other College users including any third parties authorised to access the College's network or computing facilities must be familiar with this Framework and any appropriate supporting documentation relevant to their role.

This Framework should be read in conjunction with the College's ICT Acceptable Use Policy, ICT Security Policy and the Data Protection Policy, and should be communicated to all users and relevant external parties.

Senior Management Team

The Senior Management Team is ultimately responsible for establishing frameworks and for issuing and reviewing policy statements and procedures to support the College with which members of the College must comply.

The Senior Management Team requires all College management staff to be accountable for implementing an appropriate level of security control for the information owned by that department and processed by persons accessing that data (the Information Asset Owners). This includes undertaking a Data Protection Impact Assessment where a type of processing, including new technologies, is likely to result in a high risk to the rights and freedoms of natural persons.

Each person is accountable to their relevant line manager as applicable for operating an appropriate level of security control over the information and systems they use to perform their duties.

Director of Digital Services/Director of Estates and Corporate Services

The Director of Digital Services and the Director of Estates and Corporate Services are responsible for the overall coordination of the management of information security from a technical and organisational viewpoint, maintaining this Information Security Framework and providing advice and guidance on its implementation. All staff have responsibility for adhering to information security requirements within their area. It is noted that failure to adhere to this Framework may result in the College suffering financial loss, operational incapacity, and/or loss of reputation. Data access or

processing that fails to observe the provisions of this Framework may result in disciplinary action.

Data Protection Officer

The Data Protection Officer (DPO) is responsible for informing, advising, and monitoring compliance with data protection legislation and related College policies and procedures. The DPO should be involved properly and in a timely manner in all data protection matters including risks associated with processing operations that may impact information security.

Risk Management Committee

The Risk Management Committee has responsibility for overseeing the management of the information security risks to the College's staff and students, its infrastructure and its information.

Glasgow Kelvin College has a responsibility to abide by and adhere to all current UK legislation as well as a variety of regulatory and contractual requirements and agreements.

7. Supporting Policies, Codes of Practice, Procedures, and Guidelines

Supporting policies have been developed (see below) to strengthen and reinforce this Framework. These, along with associated, procedures, standards and guidelines are published together and are available for viewing on the Glasgow Kelvin College website.

All staff, Board Members and other College users, including any third parties authorised to access the College's network or information system facilities are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.

Supporting Policies/Procedures:

- ICT Security Policy
- ICT Acceptable Use Policy

Information Security Policies, Procedures and Guidelines:

- ICT Acceptable Use Policy
- ICT Password Change Procedure
- ICT Security Policy
- Social Media Procedures
- Data Protection Policy
- College Data Privacy Notices
- Data Subject Access Request Procedure
- Data Protection Impact Assessment

- Data Breach Reporting Procedure
- Data Retention Schedule

This Framework has been developed with due regard to all relevant legislation including:

- Computer Misuse Act 1990
- UK GDPR
- The Data Protection Act 2018
- Freedom of Information (Scotland) Act 2002
- Regulation of Investigatory Powers Act 2000
- Defamation Act 1996
- Obscene Publications Act 1959 and 1964
- Prevent Duty Guidance (Scotland)
- Protection of Children Act 1978
- Criminal Justice Act 1988
- Criminal Justice and Immigration Act 2008

8. Compliance and Breach of Policy

The College shall conduct cyber security compliance and assurance activities, facilitated by the College's ICT Services Team to ensure cyber security objectives and the requirements of the College policies are met. Wilful failure to comply with the aforementioned policies will be treated extremely seriously by the College and may result in disciplinary action.

9. Review and Development

This Framework, and supporting documentation, shall be reviewed and updated every three years or sooner if required to ensure that they:

- remain operationally fit for purpose
- reflect changes in technologies
- are aligned to industry best practice
- support continued regulatory, contractual and legal compliance

Changes to this framework will be presented to the Senior Management Team for review prior to publication.

If you have any questions regarding this framework, please contact: Jason Quinn, Director of Digital Services - JQuinn@glasgowkelvin.ac.uk or Lisa Clark, Director of Estates and Corporate Services – lisaclark@glasgowkelvin.ac.uk