Policy Number	CPP 007
Level	3
Issue	1
Issue date	21/01/2021
Review Date	26/11/2023
Author	N.Murton
SMT approval	26/11/2020

Edinburgh College

For the future you want

Information Security Classification Policy

Corporate Development

1. INTRODUCTION

Why do we need an Information Security Classification Policy?

Edinburgh College holds a wide range of information and has a legal responsibility to manage all information in its care to ensure that risk is minimised; to ensure business continuity and to protect the rights of individuals.

All information the College collects, stores, processes, generates or shares to deliver learning and teaching and associated support services; and to conduct wider business activities, has intrinsic value and requires an appropriate degree of protection.

Everyone who works within Edinburgh College (including staff, contractors and service providers) has a duty of confidentiality and a responsibility to safeguard any College information or data that they access, irrespective of whether it is marked with an information security classification or not.

Edinburgh College Security Classifications have been developed to provide the College with a foundation to assist colleagues in deciding how to share and protect information. Four simplified levels of security classifications for information are now set out in this policy (section 5).

The new levels are discussed in section five below.

The simplified classification provided by this policy will be used to create an I*nformation Labelling and Handling Procedure*, co-designed with colleagues, which will make it easier and more efficient for information to be handled and protected, whilst placing greater emphasis on colleagues taking personal responsibility for data they handle.

2. POLICY

In line with Edinburgh College's Information Security and Breach Policy and Data Protection Policy, it is the College's policy that:

- Information should be both secure and available to those with a legitimate need for access in accordance with its classification level;

- Access to information will be on the basis of least privilege and need to know;

- Information will be protected against unauthorised access and processing in accordance with its classification level;

- Information Assets ***Owners*** shall be identified for all College Information Assets;

- Information shall be ***classified*** to an appropriate level on the basis of:

    - the risk presented by its inherent confidentiality; and its integrity and availability requirements; and
    - in accordance with all relevant legislative, regulatory and contractual requirements.

- Information (individual documents) and Information Assets shall be ***labelled and handled*** according to how critical and sensitive they are; and

- ***Labelling and Handling Rules*** (controls) for acceptable use of all Edinburgh College Assets shall be developed, publicised and implemented.

3. KEY TERMS

Information: "data, ideas, or thoughts irrespective of medium" (e.g. individual documents and files).

Document: "recorded information or objects that can be treated as individual units. The smallest unit of filing. Any piece of written information in any form" (e.g. word or excel file, an email, a voice mail message).

Information Asset: "a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles". (e.g.

Student Record System; a folder containing an entire class's Personal Learning Support Plans).

Information Security: preservation of the confidentiality, integrity and availability of information.

Information Asset Owner: a senior member of staff (head of department/faculty) who is the nominated owner for one or more identified information assets of the organisation. It is a core information governance requirement that all Information Assets are identified and that the business importance of those assets is established.

Confidentiality: the concept that information is not made available or disclosed to unauthorised individuals, entities, or processes.

Integrity: the concept that information is accurate and complete.

Availability: the concept that information is accessible and usable upon demand by an authorised entity.

4. RESPONSIBILITIES

Heads of Department/Faculty

Heads of department/faculty are Information Asset Owners for all College Information Assets.

Heads of department/faculty, as Information Asset Owners, must:

- Ensure the classification of the information they are responsible for;
- Ensure that their staff are aware of, and have confirmed, their understanding of the handling rules;
- Maintain an up-to-date inventory of information assets;
- Monitor compliance against the information handling rules;
- Review classification at least annually through EC Performance Review.

All staff

All staff must:

- Handle information appropriately and in accordance with its classification level;

- Abide by any contractual requirements, policies, procedures or systems for meeting those responsibilities; and

- Report any breaches of confidentiality, integrity or availability to the Data Protection inbox, immediately, via DataProtection@edinburghcollege.ac.uk in line with the College's Data Breach Reporting Procedure.

Information Governance Group

The College's Information Governance Group has responsibilities for developing an appropriate labelling and handling plan for College Information Assets in line with Information Security Classification Policy.

5. EDINBURGH COLLEGE SECURITY CLASSIFICATIONS

Table 1: EC Information Security Classifications

Information Classification	Description	Example Controls	Colour
Confidential (top confidentiality level)	Information has significant value: unauthorised disclosure/dissemination would lead to severe financial/reputational damage to EC.	Only those who explicitly need access must be granted it, and only to the least degree in order to do their work. (Need to know and least-privilege principles)	Red
Restricted (medium confidentiality level)	Disclosure/dissemination of this information is not intended = may cause some negative publicity, but is unlikely to cause	Only valid log-ins from small group of staff allowed	Amber

	severe financial or reputational damage.		🟧
Internal use (lowest level of confidentiality)	Information that can be disclosed or disseminated by its owner to appropriate members of our organisation, partners and other individuals as appropriate	Owner to disclose as they see appropriate.	Yellow
Public (everyone can see the information)	Information that can be disclosed or disseminated without any restrictions on content, audience or time of publication.	Disclosure must not violate any applicable laws or regulations. Modification must be restricted to individuals explicitly approved by Information Owners to modify that information.	Green

6. DIRECTLY RELATED LEGISLATION

Data Protection Law – *Personal Data* contained within Information Assets

A key principle of the General Data Protection Regulation 2016 (Article 32) is that the College must process personal data securely by means of 'appropriate technical and organisational measures' - this is known as the 'security' principle.

Article 32 turns what is considered good Information Security practice into a legal minimum and introduces established information security concepts into data protection legislation, including:

- managing, limiting and controlling access to personal data; and
- protecting the classic 'CIA triad' (confidentiality, integrity and availability) of personal data;

Under Article 32 the College must:

- assess its information security risk and implement appropriate technical controls;

- put in place appropriate technical and organisational measures to ensure a level of security of both the processing and your processing environment – this includes classifying, labelling and handling information assets.

Records Management under the Freedom of Information (Scotland) Act – *Records* contained within Information Assets

Under Scottish Ministers' Section 61 Code of Practice on Records Management under the Freedom of Information (Scotland) Act 2002, the College is required to:

- Ensure storage arrangements, handling procedures and arrangements for transmission of *records* reflect: accepted standards and good practice in information security

IS027001:2013 – Information Security Management Standard

As part of the College's commitment to meeting its Information Security (including cyber security) commitments under the Scottish Government's Public Sector Cyber Resilience Action Plan Edinburgh College is moving to meet the requirements of ISO 27001:2013, an internationally recognised information Security Management Standard.

Table 2: ISO 27001:2013 A.8.2 Information Classification Requirements

A.8.2 Information Classification		
Objective: To ensure that information receives an appropriate level of protection in accordance with its important to the organisation		
A.8.2.1	Classification of information	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.
A.8.2.2	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organisation.
A.8.2.3	Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organisation.

The College's Information Security Classification Policy, Information Security Classifications, and supporting labelling and handling plan for staff, position the College to meet the requirements of ISO 27001:2013.

7. RELATED DOCUMENTS

- Edinburgh College Information Security and Breach Policy
- Edinburgh College Data Protection Policy
- Edinburgh College IT Facilities Acceptable Use Policy
- Edinburgh College Data Breach Reporting Procedure

8. POLICY GOVERNANCE AND REVIEW

The accountable officer for this policy is the Head of Communications, Policy and Research, who will review this policy through the Information Governance Group and Senior Management team on a tri-annual basis, prior to the beginning of each academic year.

Responsibility for implementing the policy sits with SMT.