Policy Number	FEIT 005
Level	3
Issue	1
Issue date	07/12/2020
Review Date	15/10/2023
Author	A. Williamson
SMT approval	15/10/2023

Edinburgh College

For the future you want

Encryption Policy

Estates Services & IT

1. PURPOSE AND SCOPE

This policy applies to all College staff handling College information (including personal data as defined under data protection law). The policy sets out the framework within which the College will manage the encryption of the information for which it is responsible, maintaining an appropriate balance between accessibility and security. This document sets out the College's policy on processing *confidential* and *restricted* information off campus or on an external network, including the use of portable and mobile equipment. Its aim is to ensure that the College complies with data protection laws and other legal obligations and that College information is protected from unauthorised access, dissemination, alteration or deletion.

The College acknowledges the need for its staff to be able to disseminate, store and, where unavoidable, transport the information they require in order to carry out their work.

The College also acknowledges that the information it manages must be appropriately secured in order to maintain its reputation for trustworthiness, to protect against damage and/or distress being caused to those that entrust the College with their data, to protect the institution from the consequences of breaches of confidentiality including possible legal and financial consequences, to avoid failures of integrity or interruption to the availability of that information and to comply with the law and any applicable contractual agreements or otherwise.

This policy applies to all information for which the College has a legal, contractual or compliance responsibility, where that information is stored or processed electronically.

This policy applies to the use of mobile devices (e.g. laptops, tablets, and smartphones), portable storage media (e.g. USB memory sticks, portable hard drives, CDs or DVDs), remote computers, or other forms of communication (e.g. websites, email and instant messaging).

This policy applies to all staff or any other person or organisation which has access to College data.

This policy complements and supports the existing **Data Protection Policy, Information Security Policy, Data Breach Reporting Procedure** and **Records Management Policy.**

2. CONSEQUENCES OF NON-COMPLIANCE

Failure to comply with this policy may result in the College revoking access to the College's systems, whether through a device or otherwise. It may also result in disciplinary action being taken against members of staff up to and including dismissal. In the case of breach of this policy by a contractor, worker or volunteer, it may lead to the termination of the engagement. This will apply whether the breach occurs during or outside of normal working hours and whether the breach takes place at a normal place of work.

3. KEY TERMS

Confidential information

Information that has significant value and where unauthorised disclosure or dissemination could result in severe financial or reputational damage, including fines. Only individuals who explicitly need access must be granted it, and only to the least degree in order to do their work. Examples include:

- Any data defined as "Confidential" under College information security classification.
- Any set of data relating to living, identifiable individuals' health, disability, ethnicity, sex, trade union membership, political or religious affiliations, or the commission or alleged commission of an offence (special category 'sensitive' data under data protection law).
- Information that would be likely to disadvantage the College in funding, commercial or policy negotiations.
- Confidential information critical to the business continuity of the College, and information held in business-critical applications.
- Any information or data that is subject to non-disclosure agreements or any other contractual confidentiality obligations.
- Information provided to the College subject to contractually binding requirements governing the use of encryption.
- Health records of any living, identifiable individual.
- Discussion papers and options relating to proposed changes to high-profile College strategies, policies and procedures before changes are announced.
- Security arrangements for high profile or vulnerable visitors, students, events or buildings while the arrangements are still relevant.
- Information that would attract legal professional privilege.

- Finance data held in Agresso and any payment card data covered by security requirements.

Restricted information

Information that is subject to controls on access, such as only allowing valid log-ons from a small group of staff. Disclosure or dissemination of this information is not intended and may incur some negative publicity, but is unlikely to cause severe financial or reputational damage. Examples include:

- Personal data as defined in Edinburgh College's Data Protection Policy. (NB. Any database containing >1000 records of restricted information should be classified as confidential).
- Any set of data relating to identifiable individuals, including, but not limited to, students, staff, and/or stakeholders.
- Any set of data relating to living, identifiable individuals that could be used for fraud or identity theft, including, but not limited to, bank account or credit card details, national insurance number, personal contact details, date of birth, salary etc.
- Information relating to members of staffs' performance, grading, promotion or personal and family lives.
- Information relating to students' programmes of study, grades, progression, or personal and family lives.
- Information that is marked as "restricted" under College information security classification.

4. REQUIREMENTS AND KEY PRINCIPLES

The following key principles underpin this policy.

If processing personal data (as defined under data protection law) on external networks or devices staff must first consider whether anonymising the information to obscure the identity of the individuals concerned would be possible. Further guidance on anonymisation can be found from the Information Commissioner's Office, Anonymisation guidance.

College information must be stored and transmitted within College managed systems (unless in exceptional circumstances).

If confidential or restricted information (as defined in Section 3) is to be processed off campus or on an external network, then it must be stored and transmitted in an encrypted form. This includes the encryption of files sent by email, data in transit held on portable hard drives, and in the case of websites or e-commerce, the use of encrypted transmission protocols such as SSL (Secure Sockets Layer). There are exceptions where access or transmission of confidential or restricted information is being conducted using College managed systems such as College managed email and cloud services. Some examples are provided below:

Activity	Do I need to Encrypt?	Notes
Using a personally owned device to store confidential or restricted information* (*see 4.10).	Yes - Device	Storage of confidential or restricted information is only allowable by prior approval from the Executive Team, who will ensure compliance with Information Governance Security.
Sending Confidential or Restricted Information to a non-College email account.	Yes	Contact the IT team if you require installation of currently approved encryption Software.
Creating a website or ecommerce site that will involve the transmission of confidential or restricted data.	Yes	Seek advice from your IT business partner in the first instance.
Storing confidential or restricted information on a portable hard disk or USB. (Use of external data storage should be a last resort. OneDrive/SharePoint should be primary).	Yes– device or files	Before using portable devices consider if there are alternative ways to store information on site or to share using College managed tools or areas
Accessing College managed systems (e.g. Agresso, iTrent) off site via College approved access routes.	No	Existing College-managed security measures will apply.
Accessing College issued email accounts off campus.	No	Existing College-managed security measures will apply.

Staff should not use *non-* College IT centralised third party hosting services, like Dropbox or Google mail/storage when processing confidential or restricted information. Staff should seek advice from the IT department regarding College approved alternatives (such as One Drive or SharePoint) or seek authorisation for alternative use by exception.

Staff should not process confidential or restricted information in public places. When accessing email remotely, staff should exercise caution to ensure that you do not download unencrypted confidential or restricted information to a non-Edinburgh College device. Please refer to College Policies on remote working or contact IT management for additional requirements for working off campus.

When sending encrypted data outside the UK, staff should have regard for the regulatory requirements in the destination country. Be aware when travelling abroad that government agencies may require you to decrypt information on entering or exiting a country. Wherever possible, avoid travelling with confidential or restricted information. Seek advice from IT management if required.

Third party hosted data, for example where external suppliers are used, including software as a service, cloud hosted solutions and third-party web-based applications will be subject to due diligence checks, to ensure they can afford an appropriate level of security for personal data (as defined under data protection law). When requested you may be required to obtain information pertaining to supplier security and encryption measures on request.

Devices

1. Laptops, smartphones, tablets – College-owned
   - All College-owned laptops, smartphones and tablets should be encrypted unless in exceptional instances where this is not deemed necessary
   - The College's centrally approved encryption solutions will be used, and all encryption keys, passwords, passphrases or other keys must be held centrally to ensure accessibility of data when required.

2. Laptops, smartphones, tablets – Personally-owned
   - Edinburgh College retains legal responsibility, under data protection legislation, and the Freedom of Information (Scotland) Act 2002, for data stored on personal devices. Staff must avoid the storing of confidential or restricted information on personally-owned devices. Where, in exceptional circumstances, this is unavoidable staff must encrypt the device using IT approved encryption standards. Staff will be

wholly responsible for the safe management of their encryption keys, passwords and any other means of access; IT staff will be unable to recover lost passwords for personally-owned devices and staff should be aware that loss of passwords or encryption keys could render data inaccessible. For this reason, you must ensure that copies of the data are maintained on College systems to protect against risks posed by data becoming inaccessible. Given the need for duplicated storage, the preference is to access data from secure locations such as OneDrive and Sharepoint. Staff must ensure files held on devices are password protected accordingly.

3. Other portable devices/removeable media
   - Portable devices such as USB sticks, portable hard drives, and recording devices are at higher risk of loss or theft so additional care must be taken to protect the physical security of these devices.
   - Wherever available, device encryption should be used ensuring that encryption keys, passwords and any other means of access are stored securely on College networks.
   - Alternatively, encrypt files that will be stored on the device.

4. Email and data sharing tools
   - Avoid sending confidential or restricted information externally by email or using email to store such information. If you must use email to send this sort of information externally, encrypt it prior to sending (see guidance in 4.3).
   - If sending unencrypted confidential or restricted information to another *internal College email account*, to include any accounts issued by the College, take extra care that you have the correct recipient, indicate in the email subject line that the email contains sensitive or confidential information so that the recipient can exercise caution about where and when they open it. This includes those invited to view documents within cloud-based storage e.g. One Drive. Password protection for internally transmitted documents is advisable and may be mandated by the Data Protection Officer in instances of recurrent errors involving incorrect recipients.
   - Ensure that any third party working with any College data that involve confidential or restricted information handles it in accordance with this policy.
   - Encryption keys, e.g. passwords, must not be communicated within the same channel as the encrypted data, for example, do not send a password within the same email as the encrypted information, or a USB stick together with the password.
   - Suspected or confirmed compromises of *personal or special category data* must be promptly reported to the Data Protection Officer via

dataprotection@edinburghcollege.ac.uk in line with the College's Data Breach Reporting Procedure and Data Protection Policy. Information Security incidents should immediately be reported to the Chief Operating Officer.

- Lost or stolen College-issued IT devices should immediately be reported to the IT management.
- Use the College's central and secure shared drives to store and access confidential and restricted information wherever possible; this helps to ensure that only legitimate users have access to it as well as ensuring it can be readily accessed.
- Use the IT-authorised remote access facilities (such as VPN or RDS) to access College data on central servers instead of transporting it on mobile devices and portable media, wherever possible.

5. WHERE TO GO FOR ADVICE

IT - itrequest@edinburghcollege.ac.uk 0131 297 9090
Data Protection Team - DataProtection@edinburghcollege.ac.uk

6. RELATED POLICIES, PROCEDURES, GUIDELINES AND REGULATIONS

Key related policies and rules:

- Information Security Policy.
- Data Protection Policy.
- Data Breach Reporting Procedure.
- Equality, Diversity and Inclusion Policy.

7. ROLES AND RESPONSIBILITIES

Senior Management Team	To ensure that their teams are made aware of this policy and any breach is dealt with appropriately.

Line Managers	To ensure that their teams are aware of this policy, the regulations on the use of IT facilities, and any other Information Security policies relevant to their work. To ensure that staff and other people with access to information, including personal data as defined under data protection law, undertake the Information Security training at the earliest opportunity. All staff are personally responsible for ensuring they complete the mandatory training. It is the line manager's responsibility to check that it has been completed. To ensure that the business processes and practices in their areas comply with the Information Security Policies and other obligations concerning confidentiality.
Information Asset Owners	To ensure that an appropriate security classification is applied to the Information they are responsible for, and that encryption of confidential and restricted information is applied where required. To ensure that the business rules covering access rights to the service are defined and maintained, and that they are compatible with the security classification of the underlying information. To ensure that the information security risks for the service are identified, assessed and addressed prior to implementation, and reviewed at regular intervals thereafter. To ensure that information assets are effectively managed in accordance with the data protection principles and Data Protection Policy. To assist with any Information Security Incident as part of the Information Security Incident Response procedures.

College staff	To assess the need for encryption, based on requirements set out in this policy and apply appropriate security measures as needed. All staff are personally responsible for ensuring they complete the mandatory training. To comply with the regulations on the use of IT facilities. To complete all required training and follow related policies and guidance. To report any breaches or suspected breaches of Information Security in accordance with the Information Security Incident Response Policy. To inform IT Services of any potential threats to Information Security.

8. POLICY REVIEW

This policy should be reviewed whenever changes affect it or every three years, whichever comes first.