Edinburgh Napier University
Information Security Classification Scheme (ISCS)

	CONFIDENTIAL	INTERNAL	OPEN
Risk Rating/Impact	High	Medium	Low
Description	Accessible by restricted members of staff or students on a need to know basis. Often containing information which is personal, sensitive, or has high financial/commercial value.	May be seen by all members of the University but would not normally be available to people outwith the University.	Information which can be viewed by anyone, both internally and externally, including students, media and the general public.
Access	Access is restricted to a small authorised group of staff who need the information to carry out their roles. Usually not releasable under FOISA due to an exemption such as confidentiality, commercial interests or data protection.	Can be disseminated within the University. However, this may have to be released to the public under FOISA.	No access restrictions. Information is widely available and can be accessed by the public.
Transfer of data	• Only to be stored in folders with restricted access. • To be shred via a secure access-controlled link if possible. • Only be transmitted electronically in an acceptable encrypted format if secure link is not possible. • Items sent by internal mail should be placed in sealed envelopes. • External postage should be signed for.	• Information may be placed in shared folders and sent via internal email.	• No restrictions.

Examples Please note: these lists are indicative, not exhaustive	• Documents containing sensitive personal data • HR data • Student data • Reserved committee business • Security information • Commercially sensitive information • Legally privileged information • Research data containing identifiable information.	• Internal correspondence • Committee papers (non-sensitive e.g. not subject to FOISA exemptions) • Internal policies and procedures • Timetables/room bookings	• Any information on the website • Information contained within the University's Publication Scheme • Information for prospective and current students • Publications • Press releases

	• Personal data must NOT be shared with third parties without a Data Sharing Agreement being in place.
	  ○ Employees and Associates/Contractors dealing with personal data must sign an Oath of Confidentiality.
	  ○ Confidential information must not be shared with third parties without a confidentiality agreement being in place.
	• The information must be retained in line with the periods set out in the relevant University Records Retention Schedule and destroyed securely as per the 'Safe Disposal of Confidential Waste' guidance.
	• Electronic information must be maintained in accordance with the University's Information Security Policies.
		• Email links to files, not attachments where possible.
		• Use Internal mail.
			• Not required.

	• Manual information must be maintained in accordance with the Manual and Physical Data Security Policy. **Storing and Processing Data** • Locked cabinets/rooms • Restricted access network areas (folders, sites, libraries, file shares) • Out of view on desks and monitors • Password protected documents/systems **Communications** • Tracked/'signed for' mail • Double envelope • Encrypt external email		

ALWAYS CONSIDER THE IMPACT OF INFORMATION LOSS AND UNAUTHORISED DISCLOSURE WHEN PROCESSING DATA

Edinburgh Napier University
Information Security Classification Scheme (ISCS)

As a University we are in the information business – we 'process', that is: receive, create, store, retain, use, re-use, update, impart, share and dispose of, massive amounts of data and information every day. This includes customer interactions, personal data, internal and external correspondence (emails, web enquiries, letters, social media, etc.), electronic files and system information, paper and hard copy documents and records, our 'product' (teaching/learning materials, feedback), confidential and other corporate data. Information is the life-blood of the institution – essential to our continuing functioning and effectively one of the biggest *assets* of the University and there are, therefore, a variety of risks associated with its management.

This document provides a framework for staff to consider risks in respect of different types of data held, used and transmitted within the University. It also provides guidance on the storage and transmittal of information based upon the level of risk.

The **risks** which have to be considered when managing information are diverse – from disclosure of personal data in breach of Data Protection legislation or retention of information beyond the time limits allowed, to a loss of information which disrupts business operations or difficulties finding information which costs time, effort and money to retrieve or even the theft of information. This can have a damaging impact on the business, causing reputational damage, financial loss, etc. and it is therefore critical that the University puts measures in place to mitigate against these risks.

Of the risks to be considered information security is by far the most important. An assessment of the sensitivity of the information and the impact if it was disclosed will determine the level of security with which the information is protected – the ISCS will assist staff with making these decisions. It can clearly be seen in the table above that disclosure of information in the high risk category would have serious consequences for the University and individuals involved, whereas information in the medium category is likely to have little or no risk of adverse impact if disclosed and that in the low risk category is freely available.

Ensuring information is protected and held securely is crucial to mitigating the risks, and work done by Information Services (IS) is key here; however it is also the **personal responsibility** of every employee and representative of the University to safeguard the information that they deal with (process). All staff are responsible for ensuring that University information is held and transmitted appropriately.

By classifying information according to its relevant Classification Type, University employees and representatives can ensure that it is afforded the appropriate level of security and minimise the risk of something going wrong e.g. a data breach. This also gives assurance to all stakeholders that the University has the necessary safeguards in place to protect the information it processes.

The document provides examples of information and data which alongside the classifications. These examples are not comprehensive, but should be sufficient to inform any consideration of sensitivity when working with information not mentioned explicitly.

Related Legislation and University policies include:

- General Data Protection Regulation 2016
- Freedom of Information (Scotland) Act 2002
- Further information is detailed on the Records Management intranet pages.
- Data Protection Policy Statement and Code of Practice
- Manual and Physical Data Security Policy
- Procedure for a Breach of Data Security
- Information Services Security Policies
- Mobile Working Policy
- Records Management Policy Statement

Please note: these lists are indicative, not exhaustive.

Document Control

Document Control Information	
Title	Information Security Classification Scheme
Version	4.0
Author	Governance Services
Date Approved	TBC – University Information Governance Group
Review Date	Biennially
Scope	All University employees and associates processing data on behalf of the University