Information Security Classification Scheme – quick reference table (Protective Marking)

Classification Type/Name	Description	Examples	Risk Rating/Impact	Security Controls (Handling)
Protected	Highly sensitive information • **Special Categories** of personal data (GDPR Art. 9). Disclosure would be in breach of the General Data Protection Regulation. • Information which is exempt under FOISA, particularly s.30 (conduct of public affairs) in conjunction with s.33 (commercial interests) and s.36 (confidentiality). Disclosure would **substantially prejudice** the interests of any person and/or organisation and would be actionable by another party.	• Disciplinary records • Any individual's medical information • Committee meeting restricted agenda items • Information related to attempted/actual security breaches • Certain committee & meeting papers/minutes (**Communication Issues section refers**)	High Disclosure of personal data would constitute a breach of the General Data Protection Regulation and action by the ICO incl possible fines High risk of substantial harm to individuals and/or the University	**T**racked/'signed for' mail. **O**ut of view. **L**ocked cabinets. **D**ouble envelope. **M**obile working – no paper, VPN only. **E**ncrypted email. **R**estricted access network areas (eg folders) or **p**assword protected documents/systems.
Confidential	Any personal and confidential information • **Any** personal data under GDPR Art.6 (FOISA s.38 applies). • Any FOISA exemption applies. • Disclosure would **prejudice** the interests of any person and/or organisation.	• Student Records • Staff Records • CCTV Recordings • Certain committee & meeting papers/minutes (**Communication Issues section refers**)	High Disclosure of personal data would breach the General Data Protection Regulation & risk action by the ICO Risk of harm to individuals and/or the University.	**T**racked/'signed for' mail. **O**ut of view. **L**ocked cabinets. **D**ouble envelope. **A**dhere to remote/mobile working policy requirements. **E**ncrypt external email. **R**estricted access network areas or **p**assword protected documents/systems.
Internal	Any information circulated within the University only, including information which is only accessible to certain employees/ groups/committee members/contracted parties.	• Internal staff communications • Information for future publication (FOISA s.26 exemption) • Timetables/room bookings • Internal only intranet pages	Medium	**A**dhere to policy requirements for remote/mobile working. **E**mail links to files, not attachments where possible. **I**nternal mail.
Public	Any information published or available publicly (in the public domain).	• Information on the University website including the FOISA MPS and public intranet pages • Leaflets/booklets	Low	**N**ot required.

ALWAYS CONSIDER THE IMPACT OF INFORMATION LOSS AND UNAUTHORISED DISCLOSURE WHEN PROCESSING DATA
Information Security Classification Scheme (ISCS)

1. Introduction

1.1 Why do we need an 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.

The **risks** which have to be considered when managing information are diverse – from disclosure of personal data in breach of the General Data Protection Regulation (GDPR) or retention of information beyond the time limits allowed in breach of the GDPR and other legislation, 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 red category would have serious consequences for the University and individuals involved, whereas information in the yellow category (3I) is likely to have little or no risk of adverse impact if disclosed and that in the green 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). The University complies with the International Standard for managing the security of information (ISO 27001:13) which sets out various requirements, one of which is that the University is required to have an ISCS in place as a security measure to ensure that information is safeguarded appropriately and the level of protection given to information assets corresponds directly with the level of risk its processing (collection/creation/storage/retention/use/sharing/disposal) poses to the institution.

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.

1.2 Strategy 20:20

Information and records are received and created by University staff members and representatives to facilitate and support business processes – they are inputs and outputs of the University's activities. Ensuring that our information assets are managed correctly corresponds directly with the objectives of Strategy 2020, namely:

Build Innovation, Enterprise and Citizenship

- Adopt a continuous improvement/enhancement approach in all that we do
- Maximise the value of our [information] assets

1.3 ISO 27001:13 states:

A.8.2 Information classification		
Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.		
A.8.2.1	Classification of information	*Control* 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	*Control* An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.
A.8.2.3	Handling of assets	*Control* Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

2. How to use the ISCS

2.1 If the information you are receiving, creating, storing, using and/or destroying (processing) is covered by the description or examples in a given category, then the appropriate classification and risk rating applies, and the applicable control measures must be used. For example, information about student's mitigating circumstances or a staff disciplinary case require a much higher level of security when being processed than a team meeting agenda or anonymised statistics.

2.2 **Description:** These have been aligned with information legislation to highlight the types of information which are riskier for the University to process and must therefore be afforded the necessary security.

Classification Type/Name	**Description**
Protected	**Highly sensitive information** • **Special Categories of personal data** (GDPR Art.9)(exempt under FOISA s.38). Disclosure would be in breach of the General Data Protection Regulation. ICO definition: "Special category data is personal data which the GDPR says is more sensitive, and so needs more protection". Information about an individual's: o Race o Ethnic origin o Politics o Religion o Trade Union membership o Genetics o Biometrics (where used for ID purposes) o Health o Sex life or o Sexual orientation • Information which is **exempt** under FOI(S)A, particularly (in the University context) that which is covered by the following sections: o s.30 – Prejudice to effective conduct of public affairs e.g. the disclosure of the information ▪ (b) would, or would be likely to, inhibit substantially- i) The free and frank provision of advice ii) The free and frank exchange of views for the purpose of deliberation: or (c) would otherwise prejudice substantially, or be likely to prejusdice substantially, the effective conduct of public affairs.

	o s.33 – Commercial interests e.g. the information ▪ (a) constitutes a trade secret: or (b) its disclosure would, or would be likely to, prejudice substantially the commercial interests of any person (including the University, and o s.36 – Confidentiality ▪ (1) Information in respect of which a claim to confidentiality of communications could be maintained in legal proceedings is exempt information (legal professional priviledge) (2) Information is exempt information if – (a) It was obtained by a Scottish public authority from another person (including another such authority): and (b) Its disclosure by the authority so obtaining it to the public would constitute a breach of confidence actionable by that person or any other person. Disclosure would **substantially prejudice** the interests of any person and/or organisation and would be actionable by another party.
Confidential	Any personal and confidential information • **Any** personal data under Art. 6 of the GDPR (FOISA s.38 exemption applies) – The information constitutes personal data as defined by Article 4 of the General Data Protection Regulation ("any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly") and its disclosure would breach the first data protection principle ("personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ") and is therefore exempt from disclosure under s.38(1)(b) and s.38(2)(a) of the Freedom of Information (Scotland) Act 2002 (FOI(S)A). • Information which is exempt from disclosure under FOI(S)A. Disclosure would **prejudice** the interests of any person and/or organisation.
Internal	Any information circulated within the University only, including Information which is only accessible to certain employees/ groups/committee members/contracted parties.
Public	Any information published or available publicly (in the public domain).

2.3 **Risk Rating/Impact:** More practical examples of the risks and how/why they occur will be included in the main document e.g. how data loss can occur, examples of how it can be disclosed/distributed in error. Guidance and links to other guidance will be provided e.g.

2.4 Control (Handling):

The University's first line of defence in protecting the information that it holds and processes is to ensure that a Policy framework is in place to ensure that employees or associates know what is expected of them and are confident that they have the tools and guidance to do their work/implement the procedures to implement the relevant policies. To compliment this, the University provides employees with training to ensure that they are aware of the risks involved and are provided with controls to mitigate the risks.

Classification Type/Name	**Security Controls (Handling)**
Protected	• Personal data must NOT be shared with third parties without a Data Sharing Agreement being in place. o Explicit consent from the Data Subject must be given to allow specific sharing of special categories of personal data to take place (or one of the other conditions for processing under Article 9 of the GDPR must be satisfied – please refer to the Information Governance Manager/Governance Services. o Employees and Associates/Contractors dealing with sensitive personal data must sign an Oath of Confidentiality o 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 • 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 Mobile working – no paper, VPN only **Communications** Tracked/'signed for' mail Double envelope

	Encrypted email
Confidential	• Personal data must NOT be shared with third parties without a Data Sharing Agreement being in place. o One of the conditions for processing under Article 6 of the GDPR must be satisfied in order for sharing to take place e.g. consent has been obtained, the data subject has been notified in a Privacy Notice, the sharing is necessary for the provision of services for which the data was supplied, etc. – please refer to the Information Governance Manager/Governance Services. o Employees and Associates/Contractors dealing with personal data must sign an Oath of Confidentiality o 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 • 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 Adhere to remote/mobile working policy requirements **Communications** Tracked/'signed for' mail Double envelope Encrypt external email
Internal	Adhere to policy requirements for remote/mobile working. Email links to files, not attachments where possible. Internal mail.
Public	Not required.

Out of view = information must be kept out of sight of unauthorised colleagues/persons e.g. PC monitors should not be visible to the members of the public and you should be aware of who may be able to see your screen when working remotely (mobile in a public place, train, bus, etc.) and that it is best to operate a 'clear desk policy' as a general rule to minimise the risk of leaving personal, confidential or sensitive information in view on your desk.

Double envelope = for both internal and external use. The inner envelope to be marked with the security classification and the outer envelope addressed only.
Encrypted email = emails being sent external to the University's network (with the appropriate data sharing arrangements) which contain Sensitive or Confidential Data MUST be encrypted. Details are available through Information Services who provide this facility.
Mobile working = Information Services provides staff with the facility to securely access the University network remotely via a Virtual Private Network (VPN) . Mobile Working Policy

2.5 Policy Framework:

This schedule forms part of the Information Governance Policy Framework which is overseen by Information Services and Governance Services. This aligns with the University Values, specifically enabling staff to be:

- **Professional**
    - Take personal responsibility
    - Use resources efficiently and effectively
    - Comply with the University's statutory obligations, policies and regulations where applicable
- **Confident and Supported**
    - Equipped to perform role

2.6 Allied 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	V2.1
Author	Governance Services
Date Approved	2015 – University Information Governance Group
Review Date	Biennially
Scope	All University employees and associates processing data on behalf of the University