UNIVERSITY OF STIRLING

Data Classification and Handling Policy

1. Purpose

This policy provides a framework for classifying and handling data to ensure that the appropriate degree of protection is applied to all data held by the University. The classification of data will help determine how the data should be accessed and handled and ensure that sensitive and confidential data remains secure.

The correct classification of data is an important to help ensure the prevention of data leaks and minimising the impact of such leaks if they do occur. As well as being good practice, it will also help ensure the University remains compliant with the requirements of the Data Protection Act (1998) and ensure effective handling of Freedom of Information requests.

This policy will explain the responsibilities of individuals and provide a consistent classification scheme to ensure that data is appropriately protected and managed throughout the University.

2. Scope

This policy covers all data or information held, in print or in electronic format, by the University including documents, spreadsheets and other paper and electronic data and should be applied by all staff, students and other members of the University. Appendix A includes a definition of data.

This policy is also applicable to associates working with the University, agency staff, data processors, third parties and collaborators working with the University. They are responsible for assessing and classifying the information they work with and applying appropriate controls. Members of staff working with these types of associates and third parties have a responsibility to bring this policy to their attention.

3. Categories

Data classification is based on the level of sensitivity and the impact on the University should that data be disclosed, altered, lost or destroyed without authorisation. The classification of all data into different categories ensures that individuals who have a legitimate reason to access a piece of information are able to do so, whilst at the same time ensuring that data is protected from those who have no right to access the information. The classification will guide the appropriate security and technical controls required to be in place.

All data owned, used, created or maintained within the University should be categorised into one of the following four categories:

- Public
- Internal
- Restricted
- Confidential

The majority of information held by the University will come under the *Public* and *Internal* categories. A smaller amount of information will be categorised as *Restricted* or *Confidential*. The *Confidential* classification should only be used in exceptional circumstances.

The table below provides details on the types of information which come into each of these categories, who should have access to this information, how the information should be stored, transmitted and the methods of disposal that can be used.

Table 1: Data Classifications and Handling requirements

	Data Classification			
	Public	**Internal**	**Restricted**	**Confidential**
Description	May be viewed by all members of the public	May be seen by all members of the University but would not normally be available to people outwith the Institution	Accessible by restricted members of staff or students on a need to know basis. Often containing sensitive personal data	Accessible only to designated or relevant members of staff due to its potential impact on the University (including financial or reputational damage) or can have an adverse effect on the safety or wellbeing of individuals.
Level of Risk if released	None	Low	Medium	High
Access controls	No access restrictions. Information is widely available and can be accessed by the public	Can be disseminated within the University. However, this may have to be released to the public under FOISA.	Access is restricted to a small group of staff who need the information to carry out their roles. Usually exempt from FOISA on the grounds of data protection	Dissemination is strictly limited to authorised personnel only. Usually not releasable under FOISA due to an exemption such as confidentiality or commercial interests
Storage of data and security	Can be stored on any device and placed on the internet. There are no restrictions on printing and copying this data, subject to copyright restrictions.	Should be stored on University network folders. Care should be taken if information is transferred to any non-Information Services managed external and mobile devices. Paper records should not be left lying around.	Information should be held within the University network in locations with restricted access and appropriate security. This includes the Research Drive on the X drive. Information should not generally be transferred to external or mobile devices but if absolutely essential then encryption must be used. Paper records should not be left unattended.	Information should be held only in restricted areas of the University network and protected with secure credentials. Paper copies should be limited and, when not being referred to, held in locked storage.

Transmission of data	No restrictions	Information may be placed in shared folders and sent via internal email.	Should only be placed in folders with restricted access. Care should be taken when emailing and acceptable encryption* used if appropriate. Items sent by internal mail should be placed in sealed envelopes.	Should only be transmitted electronically in an acceptably encrypted format*. Hard copies of documents should be hand delivered internally. External postage should be signed for.
Disposal	No restrictions. Recycle where possible.	Most paper documents can be placed in paper recycling. Delete electronic media when no longer required	Shred or use confidential waste bags for paper documents, ensure electronic media is wiped clean	Shred paper documents and permanently destroy electronic media
Examples of data	• Any information on the website • Information contained within the University's Publication Scheme • Information for prospective and current students • Publications • Press releases • Published research report	• Internal correspondence • Committee papers • Internal policies and procedures	• Documents containing sensitive personal data • HR data • Student data • Reserved committee business • Draft reports, papers, policies • Financial information (not disclosed in Financial Statements) • databases and spreadsheets containing personal data • data on research participants	• Confidential commercial contracts • Passwords • Disciplinary proceedings • Security information • Legally privileged information • Medical records

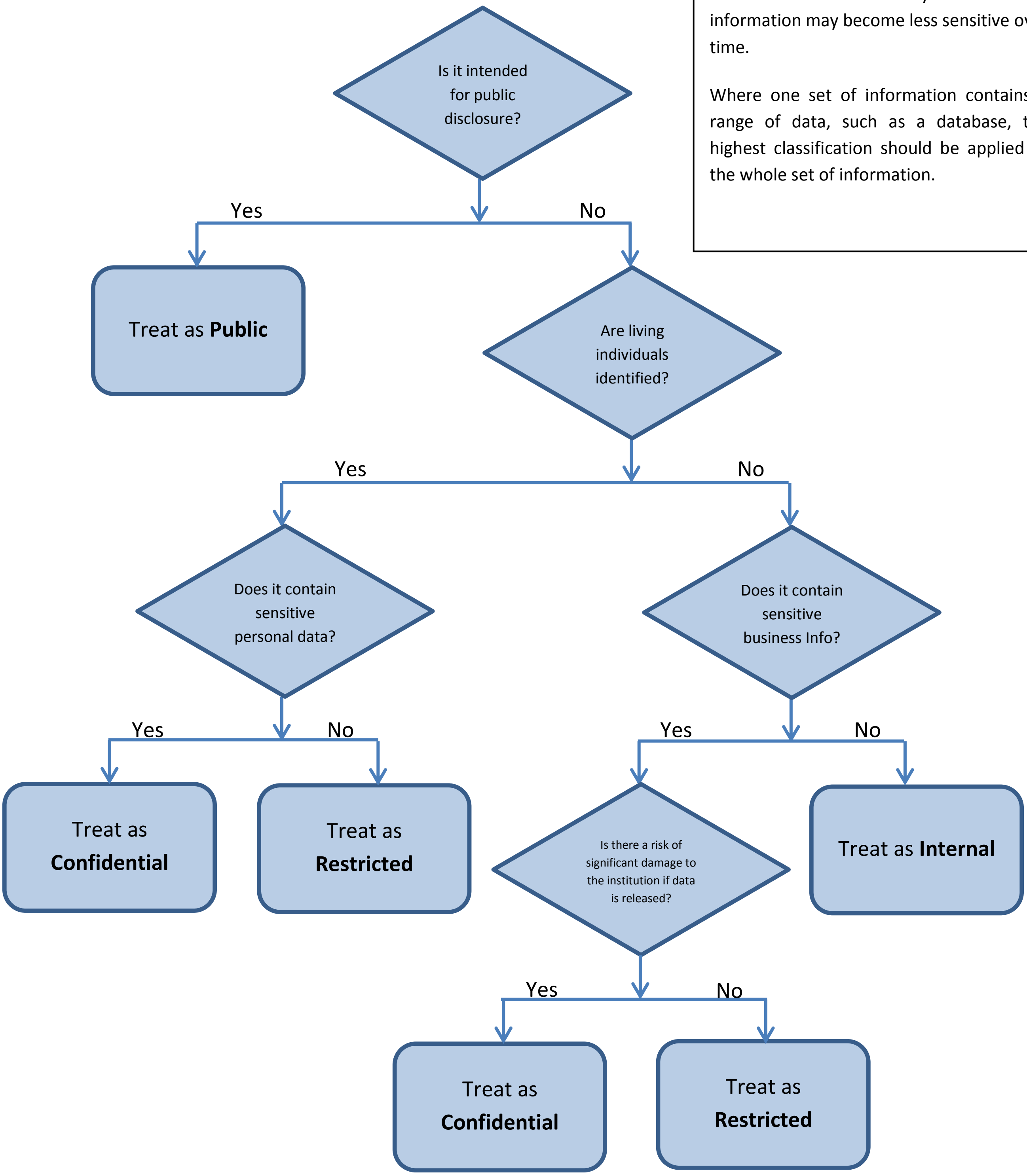
FOISA = Freedom of Information (Scotland) Act 2002

** Encryption advice can be found at :tbc*

Flow chart for determining Data Classification

This Flow Chart should be used to help determine which data classification each piece of information should be classified as. Note that it is possible for one piece of information or document to have different classifications throughout its life time. For instance commercially sensitive information may become less sensitive over time.

Where one set of information contains a range of data, such as a database, the highest classification should be applied to the whole set of information.


Is it intended for public disclosure?
Yes
No
Treat as **Public**
Are living individuals identified?
Yes
No
Does it contain sensitive personal data?
Does it contain sensitive business Info?
Yes
No
Treat as **Confidential**
Treat as **Restricted**
Yes
No
Is there a risk of significant damage to the institution if data is released?
Treat as **Internal**
Yes
No
Treat as **Confidential**
Treat as **Restricted**

4. Responsibilities/ownership

All data or information should have an owner. This could be the author of a document or the Faculty or Service area responsible for the data or information. This also applies to inter system links which pass data between systems.

It is acknowledged that it is not feasible to mark every single document in the University with the appropriate data classification. However, it is the responsibility of all members of the University to have an awareness of the four data classifications and the way information within each category should be handled. For the majority of information it is likely to be obvious by its nature which category it should come within. Where there is a possibility of ambiguity over the status of the document it is the responsibility of the data owner to ensure that the document or data is clearly marked and/or they make anyone who has access to the information aware of its status. This is particularly the case for *Restricted* and *Confidential* information which should where practicable be marked. Whilst this in itself does not make the information secure it assists with appropriate information handling.

All members of the University have a responsibility to protect University data.

5. Data Protection Act (1998)/Freedom of Information (Scotland) Act 2002

Data Protection

The Data Protection Act places obligations on the University to process personal information securely and that the appropriate technical and organisational measures are taken to prevent unlawful processing of personal data and against accidental loss, destruction or damage to personal data.

The Data Protection Act also defines *Sensitive Personal data* which relates to racial or ethnic origin, religious beliefs, physical or mental health, sexual life, political opinions, trade union membership, or the commission or alleged commission of criminal offences. The processing of *Sensitive Personal data* is subject to additional, more stringent conditions as detailed in Schedule 3 of the Act.

For further information about Data Protection please see the Data Protection Policy & Guidance.

Freedom of Information

The Freedom of Information (Scotland) Act (FOISA) requires the University to make information it holds publically available. Some information is made available as a matter of course through the Publication Scheme. Other information would be available on request. Most of the information categorised as *Internal* would be released to the public if a written request for the information were received by the University. There are exemptions within FOISA which mean that there is some information which the University is not required to release. Examples of exemptions include information that contains personal information, confidential information, commercially sensitive information, information which could endanger the health and safety of an individual etc.

For further information about Freedom of Information please see the Freedom of Information Guidance.

6. Other relevant policies

This Data Classification and Handling Policy should be read in conjunction with other relevant policies including:

- IT Security Policy (under development)
- Data Protection Policy & Guidance
- IT Use Policy
- Records Management Policy
- Freedom of Information Guidance
- Publication Scheme
- Research Data Management Policy
- Higher Education Copyright Licence.

For further information about this Policy or to report any issues relating to inappropriate data classification or handling please contact:
Deputy Secretary or
Director of Information Services

Author:	Policy & Planning and Information Services
Data Policy approved:	15 December 2014 by Court
Last updated:	May 2016
Version:	1.1
Data Classification:	Public

Appendix A

Definition of data:

This covers all data, including research data, or information held by the University, on paper or in electronic format, including documents, spreadsheets and other data. It includes data held inside systems and databases, produced by systems and data to be keyed in/loaded into systems, as well as email content.

There are further detailed definitions of administrative data at:

http://www.adls.ac.uk/adls-resources/guidance/introduction/

In addition, the University's definition of research data is at:

http://www.stir.ac.uk/is/researchers/data/introduction/