University of St Andrews

University information classification policy: implementation guide

Document type	**Guidance**
Scope (applies to)	Staff and students
Applicability date	17/02/2020
Review / Expiry date	17/02/2025
Approved date	11/03/2020
Approver	Vice-Principal
Document owner	Head of Info Assurance & Governance
School / unit	Office of the Principal
Document status	Published
Information classification	Public
Equality impact assessment	None
Key terms	Information governance and management/Information security
Purpose	Guidance on how to implement and work with the University information classification policy

Version number	Purpose / changes	Document status	Author of changes, role and school / unit	Date
2.0	Re-publication following periodic review	Approved	Head of Information Assurance and Governance, Office of the Principal	17/02/2020

1. Implementing the University Information Classification Policy

This implementation guide must be read and used in conjunction with the University Information classification policy.

In general, the classification given to information and the associated protective marking label that is applied, is a shorthand way of signalling how information is to be handled and protected.

This guide:

- Provides guidance and tips on how to classify information accurately and consistently;
- Details when information should not be classified;
- Details how protective marking labels should be applied to physical and electronic documents;
- Details how information (in physical and electronic formats) is to be handled and managed depending on its classification i.e.
    - Secure use;
    - Storage;
    - Transmission and
    - Destruction.
- Advises where further help and advice is available.

2. The University's information classification scheme

The University's information classification scheme has four levels:

- **PUBLIC**;
- **INTERNAL**;
- **CONFIDENTIAL**; and
- **STRICTLY CONFIDENTIAL**.

Each level of classification indicates the level of protection that must be given to the information. The higher the level of protective marking, the more care must be taken when handling and managing the information.

3. Selecting an information classification

APPENDIX A provides a definition of each information classification level and examples of documents/records that fall into each level.

Classification

- The creator of a document, record, or communication etc. should determine the initial classification level for that item.
- APPENDIX A of this implementation guide provides direction on how to classify information. It is important to follow the direction provided in APPENDIX A as this will support consistent classification. Definitions of each classification level are provided (these mirror those provided in the Information classification policy). Examples of the range of documents, records etc. that would routinely fall within a classification level are also given.
    - If the information in question clearly falls within one of the classification levels as defined in APPENDIX A, then that level of classification must be applied
- A risk based approach should be followed when determining the appropriate level of classification. The following factors should be considered:
    - The harm test – how sensitive is the information? If the information were to be released deliberately or accidentally into the public domain, what level of harm may arise? Is harm hypothetical or more likely than not to occur?
    - Restrictiveness – Too high a marking will incur unnecessary cost and will place restrictions on the use of information. This may mean that applying the handling/management restrictions could impede legitimate uses of the information. Conversely, applying too low a classification may mean that people and the University are placed at risk, where harm arises as a result of the information not being adequately protected.

- The current information lifecycle (draft - finalised documents) – Information classification should be driven by an evaluation of the risk associated with unauthorised disclosure at each stage of a document's life cycle.
    - Information contained within draft and/or early concept documents often has a higher degree of sensitivity, notably when there is a free and frank exchange of information, for the purposes of deliberation and decision making. Once a document has been finalised and is ready for distribution to its intended audience (perhaps by a committee or management team following approval) the sensitivity of the information may have reduced, requiring a lower level of classification.
- Review the classification applied to similar documents/records that have been classified recently (within the last 12 – 18 months) – this can act as a good initial guide. Then refer to APPENDIX A to confirm what the classification should be.
- Discuss with your line manager or seek advice – see Section **9 Contacts/ further information**.

4. Applying protective marking

General points

- Where an item is to be protectively marked, the label should displayed prominently, so that the person using an item is clear as to the sensitivity of the information contained therein.
- The creator of the document **must** apply the protective marking label.
- To differentiate between the protective marking label and an incidental use of words, protective markings should always be displayed in UPPER CASE and where the formatting of the communication allows in **bold** typeface.

Circumstances where no protective marking is required

Where information is classified PUBLIC no protective marking is to be applied.

Protective marking labels

These are:

- INTERNAL;
- CONFIDENTIAL; and
- STRICTLY CONFIDENTIAL

Applying protective marking to an electronic document, business intelligence report

The protective marking should be clearly displayed on the top of each page of the document – normally as part of the document header.

Formatting

The label should be left justified, in UPPER CASE, font style bold, with a font size no less than 9 points.

Applying protective marking to electronic documents where this is not possible to do so on each page

Where possible this should be added to the metadata / item properties for a document.

Applying protective marking to a physical folder, binder, bankers box etc.

The protective marking should reflect the marking for the **highest** level of protectively marked information contained within the folder etc.

Formatting

The label should be prominently displayed in UPPER CASE and font style bold. If the protective marking labels are hand written, pencil must not be used.

Applying protective marking to an email

The protective marking should be clearly displayed in the subject line of the email. While Microsoft outlook has the functionality to add a security setting to email communications, if that facility is applied, the label that is generated may not be visible when the communication is read via a non-Microsoft email facility. It is important that the protective marking label is included in the subject line.

Formatting

The label should be the first element of the subject line, in UPPER CASE.

5. Changes to information classification over time

The sensitivity of some information can change over time, for example once information has been released into the public domain or when a document is no longer draft, where a final approved version is available. There may be occasion when information should be re-assessed and where appropriate re-classified. As the costs associated with protecting information and the handling restrictions that accompany materials classified as **CONFIDENTIAL** and **STRICTLY CONFIDENTIAL** are high. Implementing unnecessary controls will result in additional expense.

6. Handling and managing items according to their protective marking

APPENDIX B details how documents and records etc. should be:

- Securely processed i.e. used;
- Stored;
- Transmitted i.e. disseminated; and
- Destroyed

as per the protective marking label assigned.

7. Methodology

The development of this implementation guide was partly informed by a review of relevant international standards i.e. BS ISO/IEC 27002:2005 *Information classification*. And an assessment of how other organizations have developed and implemented information classification policy.

8. Review

This implementation guide will be reviewed at regular intervals. The review period will be recorded on the accompanying coversheet. Any significant change to the University Information classification policy, the definition of personal and/or sensitive personal data, or University Policy or procedures primarily concerned with information *confidentiality, integrity and availability* may trigger an earlier review.

9. Contacts/further information

Enquiries regarding this implementation guide and/or the Information classification policy can in the first instance be directed to the University Associate Chief Information Officer (Information Assurance & Governance).

10. APPENDIX A

INFORMATION CLASSIFICATION LEVEL	DESCRIPTION	EXAMPLES
PUBLIC	Information that can be disclosed or disseminated without any restriction on content, audience, time of publication. Disclosure or dissemination would not breach any relevant laws (notably privacy) or a duty of confidence. This will include information that is published in the University web site and all content that is made available through the University Freedom of Information publication scheme. **Notes** The University is required to publish a *guide to information*. This details information that can be placed into the public domain as a matter of routine, via the University freedom of information publication scheme. The *guide to information* can also act as a useful reference when considering if it may be appropriate to classify information as PUBLIC.	• Course information • Degree congregation programme (including list of graduates) • Map of University buildings • Opening hours • Press releases • Published research papers • University prospectus
INTERNAL	Information that would only be made available to a person once they became a student or a member of staff at the University. The information would not be released into the public domain, without some form of scrutiny, to establish that release would not cause any harm. Internal information will not necessarily be made available to all members of the University community. Information may be restricted to a specific subset(s) of the University. e.g. Research grant information may be restricted to a Head of School, the research team and finance.	• Budget information • Details of funding settlements • Draft documents (which do not contain personal or sensitive personal data) • Internal audit reports • Internal memos • Key performance indicators • Lecture materials • Minutes of University and School committees • Planning applications • Staff contact details (where these do not concern public facing roles) • Statistics • Student/staff photographs

CONFIDENTIAL	Information that if subject to unauthorized disclosure, dissemination or loss could result in: a) An unwarranted breach of a person's privacy, which more likely than not would cause a level of harm and/or inconvenience. This will certainly include information that the DPA defines as personal data. Personal data is information that identifies a living individual and relates to them in a significant biographical sense. This can also include opinions formed by the University on an individual and the University's intentions towards an individual. b) Disruption to day-to-day operations of the University, where disruption only affects a sub-set of the University community. c) Damage to commercial relationships. d) Loss of competitive advantage.	• Commercial contracts • Contracts of employment • Disaster recovery / business continuity plans • Documentation that contains decisions surrounding academic progression • Examination results • Payroll / banking details • Planning / forecasting reports • Procurement / invitation to tender documentation • Research grant applications • Strategic planning • Student transcripts • University Risk Register and controls • Passwords and other forms of access control credentials
STRICTLY CONFIDENTIAL	Information that if subject to unauthorized disclosure, dissemination or loss could result in: a) Significant, unwarranted breach of a person's privacy, which more likely than not would cause substantial harm. This will certainly include information that the DPA defines as sensitive personal data. Sensitive personal data is information that concerns an individual's: • Racial or ethnic origins; • Political opinions; • Religious beliefs or beliefs of a similar nature; • Trade union membership; • Physical or mental health condition; • Sex life; • Involvement in any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings; and	• Accident reports • All medical information e.g. occupational health records/reports, fitness to work notes • Case files and correspondence surrounding investigations by a Regulatory body e.g. SPSO • Communications with Government (Ministerial level) • Communications with legal (counsel) • Communications with Police Scotland (operational matters) • Counselling records • Disciplinary proceedings • Grievance proceedings • Legal proceedings

	• Outcomes of criminal convictions. b) Substantial risk to the health, safety and wellbeing of individuals or groups. c) By prejudicial to the prevention or detection of a crime or to the apprehension and prosecution of an offender. d) The University being exposed to a civil claim for breach of confidence. e) Information protected by legal professional privilege, including legal advice privilege and litigation privilege. f) Significant financial loss (>£100,000) to the University through: • The revocation of a contract(s) for research or services; • Where information could be subsequently denied to the University, where the effect of that loss is critical business processes cannot run, or these are significantly impeded; and • Fine(s) set by a regulator.	

11. APPENDIX B

Physical				
	Use/processing	**Storage**	**Transmission/dissemination**	**Destruction**
Public	No restrictions	No restrictions	No restrictions	• Recycling
Internal	No restrictions – other than appropriate degree of caution when home working e.g. close files/documents when not in use.	No restrictions	Normally restricted to members of the University community	• Recycling
Confidential	**General use** • Always locked filing cabinet/drawer at end of working day • Exercise reasonable controls when home working or when working in a social space e.g. a local library - do not leave files/documents unattended, secure when not in use. **Public transport** • Materials should not be accessed when on public transport	Secure storage • Locked filing cabinet/drawer within a locked room or building • Always physically secure when in transit e.g. locked attaché case • Appropriate third party storage	• Distribution on a strictly need to know basis **Facsimile (fax)** • Prohibited **Internal mail – requirements** • Use double envelope – protective marking label to be present on the inner envelope only. Both envelopes should be addressed **External post – requirements** • Details of addressee to be verified and cross-checked • First class delivery and/or consider a form of recorded delivery • Use double envelope – protective marking label to be present on the inner envelope only. Both envelopes should be addressed	Irreversible destruction • Cross-shredding • Incineration • Use of certified contractor
Strictly confidential	**General use** • Always locked filing cabinet/drawer when not in use **Public transport** • Materials should not be accessed when on public transport **Home working**	Secure storage • Locked filing cabinet/drawer, within a locked room or building • Always physically secure when in transit e.g.	• Distribution on a strictly need to know basis **Facsimile (fax)** • Prohibited **External post – requirements** • Details of addressee to be verified and cross-checked • Using bonded courier or a form of guaranteed tracked delivery	Irreversible destruction • Cross-shredding • Incineration • Use of certified contractor

	• Use of strictly confidential materials outwith the University should be minimised – where home working is necessary do not leave files/documents unattended, secure when not in use.	locked attaché case • Appropriate third party storage	• If using Royal Mail special delivery is the preferred mode of carriage – this is a mandatory requirement when only the recipient of the information is to have sight of the contents • Use double envelope – protective marking label to be present on the inner envelope only. Both envelopes should be addressed **Internal mail – requirements** • Use double envelope – protective marking label to be present on the inner envelope only. Both envelopes should be addressed **Public transport** • Materials to be transported in locked container e.g. attaché case	

Electronic				
	Use/processing	**Storage**	**Transmission/dissemination**	**Destruction**
Public	No restrictions	No restrictions	No restrictions	• Normal file deletion processes
Restricted	No restrictions – other than appropriate degree of caution when home working o working in social spaces e.g. close files/documents when not in use.	No restrictions	Normally restricted to members of the University community	• Normal file deletion processes
Confidential	**General** • Information can only be used for the strict purposes for which it was created/received • Information can only be used by University employees (valid employment contract) or authorised third parties	**Home working – using personally owned equipment** • No information to be held on devices that are not owned or under the	**General** • Distribution on a strictly need to know basis **Voice-mail** • No information to be left on a voice mail message **Email** • Encrypt message and/or attachment	• University guidelines on secure electronic destruction to be followed

	• University encryption policy to be followed at all times • Laptop use – University owned preferred • Handset/tablet – University owned preferred. If privately owned, device must be wiped remotely where this is reported or stolen. Device(s) to be secured by PIN code • University collaboration tools e.g. Microsoft SharePoint to be used where possible **Home/social working – using personally owned equipment** • Preferred option: Files to be accessed and used over University VPN facility • Home devices to be encrypted, where VPN not used • Anti-virus and malware protection to be installed and up to date • When using public wi-fi services use of University VPN service required – University files should not be accessed from Cloud services **Public transport** • Information should only be processed when this is not in sight of others **Third-party cloud provider e.g. Drop box** • Third-party data processing contract must be in place before information is passed into a cloud service. Email dataprot@st-andrews.ac.uk	control of the University **Portable storage devises (USB etc.)** • Only permitted where devices are, encrypted with University approved software **University file-share or similar** • Store in appropriate file share, being mindful of the level of access to the share		

Strictly confidential	**General** • Information can only be used for the strict purposes for which it was created/received • Information can only be used by University employees (valid employment contract) or authorised third parties • University encryption policy to be followed at all times • Laptop use – University owned preferred • Handset/tablet – University owned preferred. If privately owned, device must be wiped remotely where this is reported or stolen Device(s) to be secured by PIN code • University collaboration tools e.g. Microsoft SharePoint to be used where possible **Home/social working – using personally owned equipment** • Should be the exception rather than the norm. • Preferred option: Files to be accessed and used over University VPN facility – those items to be saved on the University network and not downloaded/saved to a home device • Home devices to be encrypted, where VPN not used • Anti-virus and malware protection to be installed and up to date **Public transport**	**Home working – using personally owned equipment** • No information to be held on devices that are not owned or under the control of the University **Portable storage devises (USB etc.)** • Only permitted where devices are, encrypted with University approved software **University file-share or similar** • Store in appropriate file share, being mindful of the level of access to the share	**General** • Distribution on a strictly need to know basis **Voice-mail** • No information to be left on a voice mail message **Email** • Encrypt message and/or attachment	• University guidelines on secure electronic destruction to be followed

	• Use of or viewing of such information on public transport is not permitted **<u>Third-party cloud provider e.g. Drop box</u>** • Not permitted, other than by approved exception. University VPN and file share services etc. to be used			

Version number	Purpose / changes	Document status	Author of changes, role and school / unit	Date
1.0	First version	Approved	C Milne, Assistance Chief Information Officer, IT Services	September 2014
1.1	Minor updates	Approved	C Milne, Assistance Chief Information Officer, IT Services	March 2015