University information classification policy

Document type	**Policy**
Scope (applies to)	Staff and students
Applicability date	17/02/2020
Review / Expiry date	17/02/2025
Approved date	04/03/2020
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	Define how people should respond to protective markings when accessing, handling, storing, transmitting and disposing of information or data that is protectively marked

Version number	**Purpose / changes**	**Document status**	**Author of changes, role and school / unit**	**Date**
2.0	Re-published following periodic review; minor changes (legislative updates)	Approved	C Milne, Head of Information Assurance and Governance	17/02/2020

1. Introduction: information classification

The protection of information and/or data through the application of an information classification system (sometimes referred to as protective marking) is one of the oldest and arguably most effective regimes available for the protection of sensitive information.

Clearly labelling information to alert people to its inherent level of sensitivity and/or confidentiality, against a predefined scale is primarily designed to help ensure that materials are only made available to those persons with a legitimate right of access. Protective markings stipulate how an organisation expects information to be protected and managed during its use, while information retains a particular classification. In that regard, an information classification will also determine how information should be handled, stored and disposed. Where the corresponding protection requirements are followed the likelihood that confidentiality will be breached should be reduced. In addition, organisations should be able to demonstrate to the UK Information Commissioner that policy and procedures are in place to reduce the likelihood of information and/or data loss. The Commissioner expects that organisations take proactive measures to reduce the likelihood of data breaches occurring.

Protective marking has traditionally been used by Government, law enforcement agencies and the military. Given the requirement to protect personal and sensitive personal data (as defined by the Data Protection Act 2018 (“the DPA 2018”)), more public sector and commercial organisations are implementing information classification schemes as part of an information assurance toolkit, to protect confidentiality and maintain legislative compliance.

2. Risk management

There are risks associated with the inappropriate handling of information that carries a high degree of sensitivity. Observance of this policy and the accompanying guidance note *Policy implementation guide: information* classification, seeks to improve the management of information whereby the likelihood of the following events occurring is reduced, along with any negative impact should they occur:

- Harm or distress to individuals or groups;
- Disruption to the University business activities and/or substantial financial loss;
- Damage to the University’s reputation and standing;
- Legal action against the University or investigations by regulatory bodies.

3. Policy objectives and scope

The objectives of this Policy are to:

- Provide a simple classification system that is capable of being applied to all information or data created or received by the University, through which an appropriate protection marking can be assigned; and
- Define how people should respond to protective markings when accessing, handling, storing, transmitting and disposing of information or data that is protectively marked.

Intended audience

This Policy applies to all members of staff and members of Court. It also applies to contractors, third-party suppliers, visitors and students on placement/internship i.e. any person(s) not employed by the University, who have been granted access to University information and/or allied information systems and services.

Where the policy applies

This Policy applies to all locations and instances where:

- Where the University is responsible for personal and/or sensitive personal data as the data controller;
- Information and/or data over which the University is recognised as the owner are accessed – irrespective of location and the ownership of the technology and the service(s) used to access

information and data that fall within the scope of this Policy. Consequently, this Policy applies to all out of office (e.g. home) working.

Information and/or data received by the University

Any legal or contractual stipulations surrounding information and/or data created by a third party, which is received and accepted by the University are to take precedence over the standards and controls set out in this Policy.

Policy statement

It is University Policy that information and data are to be protected, in part by means of classification and the application of corresponding protective marking. Information and data are to be classified on the basis of the inherent sensitivity of the information or data. Each class of protective marking will have a defined set of management controls. These will determine the protections and/or conditions to be applied when a class of information or data are to be accessed, handled, stored, transmitted and disposed.

Legislative and regulatory framework

The University is responsible for protecting information and data that identify and relate to living persons, as per the provisions of the DPA 2018. Protecting personal data, through a protective marking scheme will assist the University in upholding the sixth data protection principal. This requires that steps are taken to protect personal data from unlawful use and accidental loss or damage.

Beyond legislative requirements to protect personal and sensitive data, information created under implied or actual conditions of confidentiality require to be protected with reference to the common law of confidence.

Freedom of Information (Scotland) Act 2002 (“the FOISA”)

All information held in a recorded format by the University is subject to the provisions of the FOISA, irrespective of the protective marking in use. While a request for information under the provisions of FOISA requires a response from the University, this does not mean that information must be automatically released where a request is made. There are many circumstances where the University can lawfully withhold information. University FOISA protocols exist to identify where it is more likely than not that harm would arise from the release of information that a request is then denied. It is important that requests for information which fall out-with business as usual are managed through the University’s FOISA protocols. A business as usual request is one where it is accepted or common practice that information will be routinely released in response to a request.

Relationship with existing University Policy and Regulation

This Policy provides overall direction and support for the protection of information and data by means of protective marking schemes. There are a number of other University policies, regulations and procedures which also provide (often specific) direction on managing the *confidentiality, integrity* and *availability* of University information and systems, notably the Information Security Policy and the Codes on the use and protection of personal and sensitive personal data. Relevant University policy and currently includes:

- The University Information Security Policy;
- Student and staff Codes on the collection and use of personal and sensitive personal data (revised annually); and
- The University Encryption Policy.

4. University information classification levels and definitions

The University’s information classification scheme contains the following 4 levels:

- Strictly confidential;

- Confidential;
- Internal; and
- Public.

Strictly confidential

This classifies information that if subject to unauthorised 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 2018 defines as special characteristic personal data or personal data relating to criminal convictions and offences i.e.:

   - 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
   - Outcomes of criminal convictions.

b) Substantial risk to the health, safety and wellbeing of individuals or groups.

c) Prejudicing the prevention or detection of a crime, or 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.

Confidential

This means information that, if subject to unauthorised 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 2018 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.

Internal

This means information that would only be made available to a person once they became a student or a member of staff at the University, which can include some forms of personal data e.g. lists of students/staff intended for use inside 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.

Public

This means 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 or a duty of confidence.

5. Implementation

The accompanying guidance note *Policy implementation guide: information* classification must be consulted and followed. This provides guidance and instruction on:

- How to classify information accurately and consistently;
- When information should not be classified;
- How protective making labels should be applied to physical and electronic documents;
- 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.
- Where further help and advice is available.

6. Responsibilities

Effective information security is a shared responsibility for all. For information security to be effective it requires the participation and support of all University staff, students and others who have access to the University's information and systems. All members of staff, students and others granted access to University information and systems have a responsibility to respond positively to this Policy. Specific responsibilities include:

Vice Principal (Governance)

- Adjudication, on steps to be taken to secure compliance with the policy.

Head of Information Assurance and Governance

- Promoting the policy and its implementation across the University;
- Ensuring that the accompanying guidance note *Policy implementation guide: information* classification is updated and is capable of supporting wider University requirements along with successful implementation of the Policy;
- Providing training and awareness;
- Working with Schools and Services to assess levels of compliance and to provide support to address any gaps.

Heads of School and Service Directors

- Ensuring that their School or Service achieves compliance with this Policy and that the information is classified and protected in line with the accompanying implementation guide; and
- Where there are gaps in the implementation of the Policy, that these are addressed (see Section 9.2 herein).

7. Methodology

The development of this Policy was partly informed by external benchmarking. This included a review of information classification policies from local authorities and higher education institutions and other public sector bodies within and outwith the UK and an assessment of the standard BS ISO/IEC 27002:2005 *Information classification*. On conducting an initial screening exercise, it was determined that implementation of this Policy would not negatively impact on any of the individual equality strands. Therefore a full Equality Impact Assessment is not required.

8. Review

This Policy will be reviewed at regular intervals. The review period will be approved by the University Principal's Office and recorded on the accompanying coversheet. Any significant change to 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. This Policy will be presented to the University Principal's Office for approval.

9. Policy breaches

Failure to safeguard information according to the requirements of protective marking

It will be a serious breach of this Policy where safeguards required for the protection of information classified as CONFIDENTIAL or STRICTLY CONFIDENTIAL as set out herein and in the accompanying guidance note are not put in place or followed with a reasonable level of care.

Failure to classify information and/or to apply protective markings

Given the volume of information created and received by the University along with other factors such as the wide array of formats of information, it is inevitable that occasions will arise where:

- Information is not considered for classification; and/or
- Protective markings are not applied.

Should significant gaps in information classification and/or the application of protective markings be identified, IT Services will work with a School/Unit to identify and agree what actions are to be taken to remedy that situation, including a timeframe for their implementation. If the agreed actions do not remedy the situation, or these are not implemented as agreed, and it is believed that the matter cannot be resolved, the VP Governance and Planning will be so advised.

In the first instance any suspicion of a breach of this Policy should be reported to the Service Desk (IT), or the Associate Chief Information Officer (Information Assurance & Governance).

10. Sanctions

Failure to comply with this Policy can introduce a range of threats to students, staff and the University (see section 2 herein). The possibility that the University would breach the DPA 2018 also increases, where protections required to maintain the confidentiality of information are not in place, and a privacy breach then subsequently occurs.

Where it is found that this Policy has been breached, this will be considered at a local level between the line manager and the member of staff etc. It is anticipated that in most instances, guidance and/or training will help to resolve any problems. In significant and/or repeated cases, it may be appropriate for the line manager to follow existing capability frameworks to resolve issues.

Failure to resolve issues (via the capability framework) may result in restrictions being placed upon access to a specified class(es) of information and/or University ICT facilities being denied (either on a temporary or permanent basis). This could include restrictions on using information outwith the University e.g. a suspension of home working. Should a serious breach occur it may be appropriate for action to be taken under the University's disciplinary procedures (as applicable).

Where contractual terms have been broken the University will review its position with that party. This could lead to termination of a contract of employment, studies, research or the provision of goods/services. Where it is believed that a criminal action has occurred, the University will also report this to law enforcement agencies. The University also reserves the right to pursue through the Courts a breach of the common law of confidence where it believes that such action is justified. This may also include the pursuit of civil damages against any third party. The University will also advise third parties of any infringements of their rights.

11. Availability

This Policy will be published on the University Website. The Policy can be made available in different formats, please direct any requests to the Head of Information Assurance and Governance.

12. Contacts/further information

Enquiries regarding this Policy can in the first instance be directed to the Head of Information Assurance and Governance.

Version number	**Purpose / changes**	**Document status**	**Author of changes, role and school / unit**	**Date**
1.0	First version (approved by University ICT Strategy and Planning Group)	Approved	C Milne, Associate Chief Information Officer, IT Services	September 2014
1.1	Minor updates	Approved	C Milne, Associate Chief Information Officer, IT Services	March 2015