1. SCOPE AND PURPOSE

1.1 This policy is a sub-policy of the Information Security policy.

1.2 This policy applies to all staff\(^1\) employed by the University and authorised users\(^2\) that have access to information and information technology provided by or through Bournemouth University (BU).

1.3 This policy sets out BU’s intent and commitment to preserve the confidentiality, integrity and availability of the information it holds on behalf of its students, staff and other stakeholders.

1.4 This policy also aims to ensure BU’s regulatory compliance, operational resilience, reputation and ability to sustain revenue.

1.5 This policy covers the topics related to access management which includes:
   a) Key Principles
   b) Information Asset Classification and Handling
   c) Classification Guidelines (Paper/Electronic Copy)
   d) Reclassification of Information Assets
   e) Sensitive Information Assets
   f) Freedom of Information

1.6 This policy helps all staff and students of BU to ensure the correct classification and handling methods are applied to their day to day activities and managed accordingly.

2. KEY RESPONSIBILITIES

2.1 All members of the University have a responsibility to protect University information.

2.2 The BU Board has delegated day-to-day responsibility for compliance with the policy to the Chief Information Officer.

---

\(^1\) This includes individuals working on a voluntary, honorary, placement or casual basis (PTHP), visiting faculty, emeritus, contractors, board members, visitors or those employed through an agency.

\(^2\) This includes all registered students (UG, PG, full and part-time) and alumni
2.3 Executive Deans of Faculties and Directors/Heads of Professional Services will be responsible for information security within their area of business and directly accountable to the Chief Information Officer (CIO) and BU Board for findings in non-compliance to this policy.

2.4 Business and System owners, including academic staff, are responsible for implementing the administrative and technical controls that support and enforce this policy.

2.5 All those outlined in 1.1 are responsible for complying by following the process and procedures that support this policy.

3. LINKS TO OTHER BU DOCUMENTS

3.1 In addition to this document and the supporting set of strategic policy documents there are several BU policies which complement this policy, as follows:
   - Data Protection Policy for Staff and BU Representatives
   - BU Acceptable Use Policy
   - System Management Policy
   - Technical Security Infrastructure Policy
   - Threat and Vulnerability Management Policy
   - Security Incident Management Policy
   - Mobile Computing Policy

Information Classification Management Policy

4. KEY PRINCIPLES

Information asset classification ensures that individuals who have a legitimate right to access a piece of information can do so, whilst also ensuring that assets are protected from those who have no right to access them.

4.1 All information should have an owner.

4.2 Information asset owners are responsible for ensuring that the classification scheme is used appropriately.

4.3 It is the responsibility of all members of the University to have an awareness of the four information classifications and the way information within each category should be handled.

4.4 Information assets should be made available to all who have a legitimate need to access them.

4.5 The integrity of information must be maintained. Information must also be accurate, sufficient for the purposes acquired or created.
5. INFORMATION ASSET CLASSIFICATION AND HANDLING

5.1 All information in the University must be classified into one of the following categories by those who own the information:
   a) Public
   b) Non Sensitive
   c) Restricted
   d) Confidential

5.2 The categories are classified as follows:
   a) Public information poses no risk and may be distributed with only one restriction. Some contact details are associated with specific job roles and responsibilities only and should not be released to the public without consent.
   b) Non-Sensitive information is low in risk and therefore inappropriate disclosure would have minimum significance. Information of this type may be shared with peers and partner organizations within the sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within the community. This information may not generally be released outside of the community. Specific legal or other reasons may require wider release.
   c) Restricted information is a medium risk and inappropriate disclosure could adversely affect BU's reputation, operation or cause distress to individuals or breach statutory restrictions. This information may generally only be shared with members of BU, and with others who need to know the information for a legitimate reason, for example to perform a contract with BU or prevent harm. This type of information requires the most suitable security controls that will ensure the appropriate distribution and its integrity are maintained. Specific legal or other reasons may require wider release.
   d) Confidential information is high risk and inappropriate disclosure could cause significant damage to the University's reputation or operations, great distress to individuals, pose a danger to personal safety or to life or impede the investigation or facilitate the commission of serious crime. It may result in substantial financial or legal penalties. This type of information may not, in general, be shared with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. It should only be shared under a very strict environment. Specific legal or other reasons may require wider release.

5.3 Much information will fall into the Public or Non Sensitive categories however, some information assets will be categorised as “Restricted” or “Confidential”, for good reason, such as personal privacy or protection of University interests.

5.4 Where there is a possibility of ambiguity over the status of the information, it is the responsibility of the information owner to ensure that the information 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. IT Services will develop appropriate functionality for BU email.

---

3 These classifications are linked to the Traffic Light Protocol (TLP) which is widely used in the Information Security community – Public matches with TLP:WHITE, Internal matches with TLP:GREEN, Restricted matches with TLP:AMBER and Confidential matches with TLP:RED
to enable information classification to be applied. Whilst this in itself does not make the information secure it assists with appropriate information handling.

5.5 Information assets owned and managed by the University that are sensitive or have value must be protected at all times. Consideration must be given to day-to-day activities, protection outside normal working hours and protection both on and off campus.

5.6 Asset Classification Categories, Type and Handling Methods should be applied in line with the Information Classification Handling Methods

6. CLASSIFICATION GUIDELINES (PAPER/ELECTRONIC COPY)

6.1 To the extent reasonably practicable, classification markings must be clearly visible on all BU information assets containing a classification of Restricted or Confidential.

6.2 Please refer to the Handling Guidelines on the Staff Intranet under Working at BU/Information Security & Data Protection/I Want To../Classify Information section for more information.

7. RE-CLASSIFICATION OF INFORMATION ASSETS

7.1 Some information assets may be re-classified from one category to another based on the content and intent of the asset and changes in context. There must be sound reasoning for the re-classification.

7.2 Responsibility for the re-classification of information assets remains with the owner.

8. SENSITIVE INFORMATION ASSETS

8.1 Responsibility for definition and to the extent reasonably practicable, marking of an information asset, remains with owner.

8.2 Information that is special category data for the General Data Protection Regulation (Regulation (EU) 2016/679) – that relating to a person’s racial or ethnic origin, political options, religious or philosophical beliefs, trade union membership, genetic data, biometric data for uniquely identifying them, health, sexual life or orientation shall be classified as Restricted or Confidential. Information about the commission or alleged commission of criminal offences shall be classified as Restricted or Confidential.

8.3 Identifying sensitive information is a matter for assessment in each individual case. Broadly, however, beyond the provisions of paragraph 8.2 above, information will be confidential if it is of limited public availability; is confidential in its very nature; has been provided on the understanding that it is confidential; and/or its loss or unauthorised disclosure could have one or more of the following consequences:

a) financial loss e.g. the withdrawal of a research grant or donation, a fine by the ICO, a legal claim for breach of confidence;

b) reputational damage e.g. adverse publicity, demonstrations, complaints about breaches of privacy; and/or

c) an adverse effect on the safety or well-being of Staff/Student(s) of the University or those associated with it e.g. increased threats to staff or students engaged in
sensitive research, embarrassment or damage to participants, benefactors and suppliers

8.4 Staff and students of BU must not remove sensitive information assets (Restricted / Confidential) from the university premises without prior agreement or consent from an appropriate authority. Electronic access to such information assets, when away from university premises, must be by secure means e.g. VPN, using only the officially supported channels.

8.5 Information assets which are considered sensitive (Restricted, Confidential) and are no longer needed or are deemed to have reached “end of life”, must be securely disposed of.

General

The Information Security policy and this sub policy are written in accordance with the Information Security Forum (ISF) Standards of Good Practice (SOGP).