UNIVERSITY of BRADFORD

Information Security Policy

Information Security

Version Control

Policy Number:	
Approved by:	Executive Board
Date Approved:	
Next Review Date:	
Version Number:	1.0
Applicable Statutory, Legal or National Best Practice Requirements:	General Data Protection Regulations (GDPR) Computer Misuse Act 1990 ISO 27001:2013 Information Security Management Standard
Equality Impact Assessment Completion Date: March 2018	If you require this policy in another format such as audio you can use the SensusAccess tool which is available by following this link: http://www.sensusaccess.com/web3/bradford If you require this policy in an alternative language, then you may wish to use a translation website such as http://www.workplacetranslation.com/ to convert the document to your preferred language.

This document can only be considered valid when viewed via the University website. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one on University website. Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

UNIVERSITY of BRADFORD

Contents

1 Introduction 4

2 Scope 5

3 Definitions 6

4 Responsibilities 6

5 Objective 7

6 Principles 7

7 Implementation & Training 9

8 Incident & Breach Reporting 9

9 Infringement 9

10 Related Policies & Standards 10

11 Policy Exemptions 11

12 Monitoring & Review 11

1 Introduction

The University recognises that information is an asset, and like any other business asset it has value and must be protected. This value is not just financial but is based on the impact on individuals and the University should this information be compromised in any way.

Information security provides a framework of policies, organisational structure, technical arrangements and operating environment used to protect the confidentiality, integrity and availability of the University's information assets.

Information and information systems underpin all of the University's activities whether they are learning and teaching, research, administration or management and, as such they need to be protected to ensure that students, staff and visitors have access to the information they need at the right time and in the right format in order to pursue their studies and/or carry out their work.

The University acknowledges the role of information security in enabling this and that security of information must be an integral part of its activity in order to ensure that the information the University manages is protected and appropriately secured.

The University's information and information systems are provided to fulfil the legitimate functions of the University and must only be used for lawful purposes. The University takes any misuse of its information or information systems very seriously.

Current legislation which has a bearing on Information Security, includes but is not limited to:

- Computer Misuse Act 1990
- Copyright Designs and Patents Act 1988
- Counter Terrorism and Security Act 2015 (in particular the 'prevent duty')
- Data Protection Act 2018
- Freedom of Information Act 2000
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended)
- Regulation of Investigatory Powers Act 2000

This policy is the primary policy under which all other technical and information security related polices reside. The University's Regulation 21 – ICT Regulations should be read in conjunction with this policy.

2 Scope

This policy is intended to assist the University to maintain the confidentiality, integrity and availability of its information and the systems used to manage, store, process, transmit and present it.

2.1 Information

This policy applies to all information and information systems for which the University has ownership and/or a legal, regulatory or contractual responsibility, whether that information is stored or processed electronically or by other means such as hard copy files (the "Information").

It applies throughout the lifecycle of information i.e. from receipt or creation, during its active use, access and transmission, through storage and eventual disposal when it is no longer required.

This policy extends to information described above which is held by the University on behalf of third parties and partners and by third parties and partners on behalf of the University.

2.2 Personnel

This policy applies to anyone authorised to access, handle, process, store, share or manage the University's information assets. This includes University staff, students, contractors and third-party agents.

2.3 Systems

This policy applies to the equipment, systems and credentials, which are used to access Information, safeguard Information Security, or could impact Information Security (Information Systems).

The policy covers, but is not limited to, any systems or data attached to the University's computer or telecoms networks, any systems supplied by the University, any communications

sent to or from the University and any data held on external systems (whether hosted in the cloud and/or on third party systems) which the University owns or has responsibility for.

3 Definitions

Availability - information is available to authorised users when and where it is needed.

Confidentiality - Access to and sharing of sensitive or personal information is restricted only to authorised individuals.

Information Asset – a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. It has recognisable and manageable value, risk, content and lifecycles. It can be in paper or digital format including hardware, software, infrastructure and third-party services (whether on-premise or hosted in the cloud). An information asset can exist in a filing cabinet, as a corporate electronic system or a folder on the H drive.

Information Security – Safe-guarding information assets from unauthorised access or modification to ensure their availability, confidentiality, and integrity.

Integrity - The preservation of the complete, accurate and validate state of information assets i.e. information can be relied upon to be accurate and reliable.

Risk - The probability of a threat exploiting a weakness or vulnerability and its resulting consequence leading to an adverse event

Risk Assessment - A process for identifying and evaluating risks

4 Responsibilities

The Executive Board is responsible for approving this policy.

This policy is mandatory for all staff, students and third parties who access the University's information. It is important that you read and understand this policy and comply with it.

The University Secretary and Director of Planning, Legal & Governance undertakes the role of Senior Information Risk Officer (SIRO) and has overall responsibility for the acceptance, or otherwise, of information risks for the University.

The Chief Information Officer (CIO) is accountable for the management and delivery of business systems, technology and information.

5 Objective

This policy sets out the framework for ensuring that:

- the security of the information for which it is responsible is managed effectively, maintaining an appropriate balance between accessibility and security.
- all those who are authorised to, can easily access all the information they need to fulfil their role.
- the confidentiality, integrity and availability of the University's information assets and information systems is maintained.
- the University's information assets are adequately protected against unauthorised access, malicious or accidental loss, misuse or damage.
- all users of University information assets are aware of and comply fully with this policy and all supplementary regulations, policies, processes, standards, procedures and guidelines.
- risks to University information assets are appropriately managed.
- information security incidents are reported promptly and managed and resolved effectively thereby mitigating against any legal liability.
- the University meets relevant audit and statutory requirements.
- there are effective business continuity and disaster recovery plans in place.

6 Principles

The University is committed to the implementation of this policy in accordance with the University values.

University data (information) will be classified and provided with appropriate safeguards ensuring it is protected against unauthorised or inappropriate access or use and against

accidental loss, destruction or damage thereby ensuring its confidentiality, integrity and availability.

The level to which Information Security controls are applied in individual circumstances shall be driven primarily by the nature of the Information concerned and consideration of the risks involved. All information (both digital and printed) should be classified and handled in line with the Information Security Classification and Handling Policy.

A defence in depth approach to Security controls will be adopted, combining a multi-layered approach to security in order to reduce any single point of failure and subsequent compromise. These security measures will consist of a mixture of people (e.g. awareness & education), process (e.g. clear policies, standards and audits) and technology solutions.

The University will adopt an information security risk management approach in line with the Institutional Risk Management Policy to ensure information security risk mitigation efforts reflect the University's risk appetite.

To reduce the risk of compromising confidentiality, integrity or availability of information assets, information security risk assessments will be carried out and information security risk registers maintained and reviewed regularly to ensure current risks are being managed effectively and any new risks are identified.

There will be an on-going information security awareness campaign to all staff and students covering essential policies and relevant responsibilities. Specialist advice on information security shall be made available to all users accessing and/ or processing the University's information. All new and existing staff will be required to complete an information security and data protection awareness programme covering risk to University information and practical measures to help protect it.

User access will be based on role requirements rather than job titles. Access rights will be reviewed at regular intervals and revoked as/ when necessary.

Third parties handling information on behalf of the University shall be required by contract to adhere to the Information Security – Third Party Compliance Policy.

Security requirements should be identified at the “requirements phase” for all new projects. These should be justified, agreed and integrated into the early stages of projects. Before system go-live, the project delivery process shall ensure that all information systems are subject to appropriate testing to ensure that risks to confidentiality, integrity or availability are managed and controlled effectively.

Disaster recovery and business continuity plans for mission critical information assets and related services will be maintained and regularly tested.

The University will monitor and audit compliance with the Information Security Policy, supplementary policies, processes, standards, procedures and guidelines.

7 Implementation & Training

The Policy will be uploaded onto the University website.

The approval of the Policy will be communicated in the weekly University staff briefing.

Line Managers are responsible for raising awareness of all new/updated policies through their normal Faculty/Directorate communication channels.

Policies will be published on the Student Portal and communicated through normal channels.

Information Services will work with Faculties/Directorates to identify appropriate provision of training, guidance and support to Line Managers on the implementation of this Policy.

8 Incident & Breach Reporting

Any data or information security related events or suspicions including:

- Any infringement of this policy;
- Any information security event (actual or suspected); or
- Technical problems, requests or concerns regarding a suspected information breach must be reported via IT ServiceNow or to the IT Service Desk on x3333 as soon as possible.

All breaches involving personal information must be reported to the Data Protection Officer in Legal & Governance in line with the Data Breach Procedure.

9 Infringement

Breach of this policy or wrongful disclosure of confidential information will be handled by the University's student disciplinary processes, defined in Regulation 28, and the staff disciplinary processes available through Human Resources.

A breach of this policy may lead to sanctions being imposed.

In cases where neither the Staff or Student Disciplinary Policy apply, i.e. where an alleged breach has been undertaken by someone who is neither a member of staff nor a student, an investigation will be conducted by the Associate Director of IT Services in conjunction with Legal & Governance.

Breach by a third party may lead to termination of contract and claim for damages.

Where an offence has occurred under UK law, it may also be reported to the police or other appropriate authority and could lead to civil or criminal proceedings.

If you need any assistance with interpreting or applying this policy, you should contact IT Services through IT ServiceNow.

10 Related Policies & Standards

This Policy, together with the subsidiary policies and implementation documents, comprise the University's Information Security Policy Framework which is supported by a number of associated regulations, policies, standards and procedures. These include, but are not limited to:

- Regulation 21 – ICT Regulations
- ICT Acceptable Use Policy
- Data Protection Policy
- Information Security Classification & Handling Policy
- Systems Monitoring Policy
- Third Party Compliance
- Incident Reporting & Management
- Regulation 28 – Student Disciplinary Procedure
- Staff Disciplinary Procedure

11 Policy Exemptions

Every effort must be made to comply with all University information security policies. Where it is not possible to apply or enforce any part of this policy, either for operational or legitimate academic reasons, a policy exemption request should be submitted through IT ServiceNow. The IT Risk & Security Manager in conjunction with the Data Protection Officer will review the business justification, advise on the potential risks involved and agree any exceptions.

12 Monitoring & Review

This policy will be reviewed annually, or as appropriate and in response to changes to legislation or University policies, technology, increased risks and new vulnerabilities or in response to security.