INFORMATION SECURITY AND MANAGEMENT POLICY

PREFACE

The data we collect, hold and use at the University of Birmingham is essential to our success in all our activities. Further it is fundamental to operational efficiency and effective decision making.

Therefore, the data generated and held by the University is an important asset that must be managed appropriately. We all manage data every day. This policy sets out the priorities:

- *Maintain SECURITY of information, data and IT systems*
- *Increase SPEED to answer questions and make better decisions*
- *Increase TRUST to use the same data for many different purposes*
- *Increase COMPLIANCE with external regulations.*

With speed and trust in our data, held in a secure and compliant way, we should be able to visibly enhance:

- *Student Experience: e.g. reliable timetabling*
- *Efficiency: e.g. collecting data once but using it many different times without cleansing or extensive manipulation*
- *Effectiveness: e.g. linking across multiple systems to see dependencies and connections*
- *Risk management: e.g. complying with new requests for data by regulators, avoiding reputational or financial damage of security breaches*

We cannot achieve these without changing our behaviours around Information, specifically:

- *Embedding baseline security and resilience into our IT systems and business processes*
- *Breaking down silos by considering data for the whole university not just local use.*
- *Stewarding data by understanding its varied uses and maintaining it to agreed standards*
- *Seeking resolution to data quality issues and actively managing the data.*

To achieve our goals, we need a transparent and rigorous approach to data and information security and management, specifically:

- *Understanding of the risks and training to enhance data awareness and capability*
- *Clear roles and responsibilities around data*
- *Visible data quality monitoring and a published report/resolution process*
- *Agreed definitions around the most important data we use*
- *Creation of venues to have a purposeful conversation around data*
- *Tools to manage data more effectively*
- *Embedded business processes to manage change and monitor and test security compliance and infrastructure.*

The key to thinking about our data differently is an understanding that data is everyone's opportunity, not a problem for a few.

The remainder of this document sets out our policy and governance framework to achieve these goals. The terms data and information are used interchangeably throughout this document.

1. PURPOSE AND GOALS

1. This policy covers the governance of data and information in all its forms, balancing utility and business value against security and risk.
2. This policy aims to maintain and improve the security of our systems and the quality of our data by improving the data capability and awareness of our staff, students, and other users of the University's data or computing and networking facilities and ensuring they are supported by appropriate tools and processes.
3. It provides clarity about their responsibilities and required activities and a framework for improving their skills and understanding and providing supporting structures and processes. Much of the improvement in how data is managed is based on changes in behaviours that are informed by a deeper understanding of how data is used across the University.
4. The impact of this policy will be a measurable improvement in IT security and data quality. We will develop tools to track and publish data security metrics and data quality metrics against our stated goals of **security**, **speed**, **trust** and **compliance**.
5. The terms 'data' and 'information' are used interchangeably in this policy, as are 'information security' and 'cybersecurity'.
6. This policy does not specifically address issues of privacy or personal data protection, although good data management and security are essential for compliance with data protection laws. Concerning privacy and data protection, the Data Protection Policy [2] takes precedence.
7. This policy is supported by subsidiary documents such as standards and procedures [4] that carry the same weight.
8. This policy will be regularly reviewed and updated to ensure it remains current.

2. REACH

1. This policy applies to all persons and corporate entities who access the University's data or computing and network facilities including students, staff, contractors, visitors and any others, in all locations where the University conducts its activities without geographical limits, subject to applicable local laws and regulations.
2. This policy applies to all forms and formats of information including electronic, optical and paper formats as well as textual and audio-visual communications.
3. This policy applies to all data owned by the University, under the University's custodianship or otherwise present in the University's network or computing environment on any of the University's premises or in any external or cloud-based IT infrastructure licenced, rented or contracted by the University or on the University's behalf.

3. PRINCIPLES

Data and information shall be managed to optimise its value to the University and reduce risks associated with non-compliance, poor data quality, and information breaches. Information security and management at the University are based on the following principles:

1. Data is a valued asset.
   - **i.** Data has value as much as other assets such as buildings, vehicles or money.
   - **ii.** Data should not be considered as belonging to individuals or units – rather it is managed by them on behalf of the University.

2. Data is managed.
   - **i.** Data should be managed appropriately (that is collected, stored, protected and used) throughout its life cycle.
   - **ii.** Data management should be seen as a core capability and part of the University's approach to 'Intelligent regulation'.
   - **iii.** Named roles with specific responsibilities for the curation of data from data entry to archive or disposal must be defined, appropriately resourced and skilled.
3. Data is fit for purpose.
   - **i.** Data shall be accurate and complete, at the appropriate quality for its primary purpose and all other known legitimate uses.
   - **ii.** Data should be monitored so it can be trusted. Data owners have the role of accountability and oversight to assure this trust, with decisions and actions recorded at an appropriate level of detail.
4. Data is accessible, comparable and reusable.
   - **i.** Data shall be made available where and when required, subject to appropriate security constraints.
   - **ii.** Standards will be consistently applied to encourage reuse, and promote a common understanding of context, meaning and comparability.
   - **iii.** Data should be easy to find, quick to understand and simple to compare.
   - **iv.** Data should be consistent and predictable, avoiding harm caused by conflicting versions.
5. Data is secure and compliant with regulations.
   - **i.** Data shall be protected against unwanted, or unauthorised access. Appropriate confidentiality shall be maintained.
   - **ii.** Data shall be acquired, used, stored and disposed of in compliance with the law and applicable standards, regulations and contractual obligations.
   - **iii.** Data integrity protects the university from reputational, financial and regulatory damage.

4. RESPONSIBILITIES

Every person to whom this policy applies has specific responsibilities and the University shall ensure that appropriate training and preparation is provided for all.

1. All individuals having access to the University's data or computing and network facilities, except for those accessing only 'guest' or publicly available facilities, are responsible for:
   - **i.** Complying with this policy, the Data protection Policy [2], the IT Code of Practice [1] and related standards, procedures and guidance appropriate to their roles.
   - **ii.** Maintaining vigilance and reporting security-related incidents and possible breaches of this policy to the IT Service Desk and notifying the Data Protection Officer in cases involving personal data, in accordance with the University's Data Protection Policy [2].
   - **iii.** Completing the Information Security Awareness and Data Protection training provided by the University.
   - **iv.** Ensuring that any data they create or amend is done with an eye to data quality and an understanding of how it may be reused, shared, and disposed of, and its importance to the overall success of the University's endeavours.

2. The **Information Security and Management Group (ISMG)** is the University's oversight committee for information security and information management. It reports into the University Executive Board and has responsibility for:

   i. Directing, evaluating and monitoring information security and information management activities.
   ii. Decision making and resolving issues and conflicts of interest.
   iii. Setting goals for security and information management.
   iv. Conducting annual reviews of this policy with onward transmission to UEB for final approval.
   v. Ensuring clear direction and visible management support for information security.
   vi. Ensuring that stakeholders are adequately represented.
   vii. Approving standards issued under this policy.

3. The **Data Management Group** shall be responsible for creating and maintaining the management structures, procedures and practices concerning Data Management (as distinguished from Information Security).

4. **Heads of College and Professional Services**, are responsible for ensuring communication of, and compliance with, this policy in their respective colleges and departments.

5. **Data Owners** are accountable to the University for data assets within their control and are responsible for approving their legitimate and appropriate business use. Data Owners are assisted by Data Stewards.

6. **Data Stewards** are responsible for day to day management of data assets under the authority of the Data Owners. They are responsible for the quality of the data under their control and assist in delivering the responsibilities of their Data Owners, working with a number of 'data doers'.

7. The **Chief Information Security Officer** (CISO), assisted by the **IT Security** team, is responsible for information security management; ensuring compliance with applicable laws, regulations and standards; managing information-related risk and driving the IT security strategy and implementation forward while protecting the University from security threats and ensuring effective management and resolution of incidents, attacks and breaches of this policy.

8. The **Data Protection Officer** (DPO) will ensure effective management and resolution, in consultation with the CISO, of incidents and breaches concerning personal data.

9. **IT Services** and other technical staff are responsible for ensuring that the services, systems and IT infrastructure under their control are set-up and managed in accordance with this policy.

5. CONTROLS

Controls shall be deployed to protect people, technology and processes from deliberate attacks, technical faults and accidents appropriately and proportionately based on assessment of risk, within the framework of an Information Security Management Systems (ISMS) compatible with ISO27001 and related standards. This includes security practices related to, or relying upon, information technology or operational technology environments and systems.

1. **Data classification:** The University shall adopt a data classification and marking scheme based on the level of risk associated with data assets. Data shall be considered confidential if it has been provided on the understanding that it is confidential or a breach has one or more of the following consequences:

   i. Reputational damage involving adverse publicity in local media over an extended period or national, international or social media coverage.
   ii. Moderate, severe or extreme service disruption, possibly over an extended period.

iii. Significant financial impact such as liability for fines and penalties, loss of earnings or reduction in value of assets.
iv. Adverse effects on the safety or well-being of members of the University or anyone associated with it. For example, threats to staff or students engaged in sensitive research or harm to benefactors, suppliers, staff or students.
v. Failure to comply with applicable laws, regulations or contractual obligations.

2. **Personal data:** Personal data that falls within the scope of privacy laws such as the Data Protection Act 2018, the European Union General Data Protection Regulation (GDPR) and successor legislation shall be considered confidential, managed accordingly as defined in the Data Protection Policy [2] and securely disposed-of when no longer required.

3. **Confidential data:** The University shall provide the controls and technical security measures required to protect data at rest and in transit as required by its classification, including:

i. Data shall be stored in centrally managed data stores rather than local hard drives or removable media, where practicable.
ii. File, database or disk encryption must be used except where compensating controls can be shown to provide an equivalent level of protection.
iii. Data transferred over data communication networks shall be encrypted or otherwise protected to University standards. This includes email and other types of electronic messaging.
iv. Paper copies and removable media should be clearly marked according to the data classification scheme and kept in locked cabinets with known key holders.
v. Removable media and mobile devices shall be protected against unauthorised access according to the level of risk.
vi. Confidential data shall be disposed-of securely when no longer required.

4. **Access control:** Data and supporting IT infrastructure and facilities must be accessible only by authorised persons:

i. The identity of all who access University systems shall be verified using an appropriate level of authentication. Where passwords are used, they must conform to University standards.
ii. Additional forms or 'factors' of authentication shall be used where appropriate, based on an assessment of risk.
iii. Access records should be kept for at least six months to allow for potential investigations and to maintain accountability for user actions.
iv. Access to data will be granted based on legitimate business need and shall be revoked on change of role, reassignment or termination.
v. Data that is classified explicitly open or public shall be made available to all without restriction or reserve.

5. **People:** Controls will be deployed to reduce the risks associated with human error, theft, fraud, nuisance or malicious misuse of facilities; including but not limited to:

i. Background verification checks, such as references, for candidates for employment, contractors, and other potential users will be carried out in accordance with relevant laws, regulations and ethics, proportionate to the confidentiality of the data to be accessed.
ii. Information Security Awareness, Data Protection and related training will be made available for all staff, and others as appropriate and supported by continuing communications and training activities.

6. **Environmental Controls:** Controls will be implemented, as appropriate, to prevent unauthorised access to, interference with, damage to, or removal of, data assets and

supporting IT infrastructure. These may include physical, technical, procedural and environmental measures including:

- **i.** Physical access to facilities storing or processing confidential data will be strictly governed to ensure that protection measures are commensurate with identified security risks.
- **ii.** Equipment will be protected to reduce the risks from environmental threats and hazards, power interruptions, and other disruptions caused by failures in supporting utilities.
- **iii.** Network security measures will be deployed to protect the University's data communications and computing facilities, including firewalls, switches and other devices, appliances and systems as appropriate.
- **iv.** Equipment will be correctly maintained to ensure its continued availability and integrity.

6. IT PROCESSES

Security and good data management shall be designed-in to all processes involved in the operation, development, maintenance, support and disposal of IT systems and services to ensure that it is a natural part of the culture and practice concerning technology and information.

1. **Operations Management:** Design, build, testing and operating procedures for information processing facilities, systems and networks will be adequately documented and sensitive operational documentation will be stored securely with restricted access, and:
   - **i.** Changes to information processing facilities and systems will be subject to formal change control procedures and records kept of all such changes for at least five years.
   - **ii.** Capacity planning and monitoring will be performed to ensure that adequate processing, storage and network capacity are available for current and projected needs, with satisfactory levels of resilience and fault tolerance.
   - **iii.** Systems and data assets will be regularly scanned for vulnerabilities and further security verification such as penetration testing will be performed where appropriate.
   - **iv.** Separation of responsibilities and restricted data transfer will be maintained between live and test or development environments.
   - **v.** Detection, prevention, and recovery controls to protect against malicious code, fraudulent activity or malfunctioning systems will be implemented. Faults and errors will be logged and monitored, and timely corrective action taken.
   - **vi.** Licensed systems will be operated in accordance with the University's Software Licensing Policy [3]**.**
   - **vii.** Third party service delivery agreements will be implemented, operated, and maintained. Such undertakings will be monitored and periodically audited.
   - **viii.** System clocks will be synchronised securely, under the control of authorised staff.
2. **Systems Development and Maintenance**: The security risk of all system deployment and development projects will be assessed, and access to data controlled. Security and good data management practices will be designed-in, including all aspects of integration with other systems.
   - **i.** Cryptographic techniques will be used, where appropriate, and the associated keying information will be protected.
   - **ii.** All new information systems, major software and infrastructure changes, upgrades and new versions will be subjected to formal security verification including vulnerability scanning, penetration testing and other measures as appropriate, before they go live and regularly thereafter.
   - **iii.** Changes affecting enterprise data will be verified to ensure compliance with good data management and security practices that protect both the security and value of data.
   - **iv.** New system deployments and significant changes will not be allowed to proceed if they expose the University to unacceptable risks.

3. **Business Continuity Management:** The University will maintain a coordinated approach to the assessment of business continuity requirements across all aspects of the organisation, and the identification of appropriate areas for further action.

   i. A formal risk assessment exercise will be conducted in accordance with ISO/IEC 27005 to classify each system according to its level of criticality to the University and to determine where business continuity planning is needed.

   ii. Business Continuity Planning will be developed with provision for each system or activity where the need has been established. The nature of the plan and the actions it contains will be commensurate with the criticality of the system or activity to which it relates.

   iii. Business Continuity Plans will be periodically reviewed, updated and tested.

4. **Incident Management:** Procedures will be established and publicised to ensure a quick, effective, and orderly response to information security, data protection and data quality incidents and breaches.

   i. Mechanisms will be put in place to enable the types, volumes, and costs of information security, privacy and data quality incidents to be quantified and monitored.

   ii. Relevant, authorised staff will be trained in digital evidence collection, retention, and presentation, in accordance with legislative or regulatory obligations.

5. **Asset Disposal:** Data assets such as laptops, desktop computers, servers, disk drives, tablets, smartphones and any other type of media or device that contains data as defined and covered by this policy must be securely and safely disposed of when no longer required in such a way as to ensure that the data is wiped or destroyed and cannot be recovered or reconstituted.

   i. Asset disposal includes, but is not limited to, the following:
      a. Disposal of unwanted IT equipment.
      b. Upgrade of office equipment, such as photocopiers, scanners, printers, fax machines or telephones that may have data storage.
      c. Replacement, due to a fault, of office equipment.
      d. Termination of contract for leased office equipment.
      e. Replacement of storage devices in any equipment for the purpose of repairing or upgrading them.
      f. Replacement/Upgrade/End of life of a hand-held mobile device provided to staff as part of a University contract.
      g. Paper copies of confidential data must be securely shredded.

   ii. Devices and media that cannot be safely wiped must be physically destroyed in a way that ensures the data cannot be recovered or reconstituted.

   iii. All service providers who acquire University data in the course of business must be contractually bound to comply with this policy as a whole and this section in particular. Such contracts must provide for regular audits and compliance checks.

   iv. Compliance will be verified periodically and the Information Security and Management Group (ISMG) will approve changes and improvements, as they deem necessary and appropriate.

   v. The Chief Information Security Officer will publish guidance on asset disposal and will provide advice and assistance via the IT Service Desk and other IT Services teams.

7. COMPLIANCE

1. This policy is approved by the University's Executive Board and is a policy as defined in University regulations.
2. Failure to comply with this policy may result in withdrawal of services, disciplinary action, prosecution or legal proceedings.
3. Temporary waivers or exceptions may be issued by the Chief Information Security Officer in circumstances where it is not feasible to comply with this policy. Waivers and exceptions will always have an end date but may be renewed if necessary.

REFERENCES

[1]. General Conditions of Use of Computing and Network Facilities	http://itsecurity.bham.ac.uk/policy
[2]. Data Protection Policy	http://itsecurity.bham.ac.uk/policy
[3]. Software Licensing Policy	http://itsecurity.bham.ac.uk/policy
[4]. Standards, procedures and guidance	http://itsecurity.bham.ac.uk/policy

GLOSSARY

Cybersecurity or Cyber security	Security practices related to the combination of offensive and defensive actions involving or relying upon information technology or operational technology environments and systems. Generally considered a subset of information security, the term is used interchangeably with information security in this document..
Data	Individual pieces of information such as amounts, dates, quantities, text etc. The terms 'data' and 'information' are used interchangeably in this policy.
Data Asset	Or 'Information Assets', any system, device or media that holds data, including computer systems, databases, disks, USB sticks, paper documents, audio-visual recordings etc.
Data Owner	Generally, a senior member of the University held accountable for defined information assets. Also known as Information Asset Owner or Data Asset Owner.
Data Steward	Responsible for the day to day management of data and data assets, stewards work under the authority of Data Owners.
Information	Data with enough context, or metadata' to give meaning (e.g. database table and column definitions). The terms 'data' and 'information' are used interchangeably in this policy.
Information Assurance	The practice managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. IA concerns all information risk, not just security risks.
Information Governance	Oversight of the management of information at an organisation, balancing utility and value against security and risk.
Information Management	The curation, organisation and management of all forms of data and information.

Information Security	General term covering the securing of information and digital systems, synonymous with 'computer security' and 'network security', covers information in any form including electronic, paper documents, audio-visual communications and records; includes cybersecurity.
ISMS	Information Security Management System - see ISO27001.
ISO27001	International standard specification for an information security management system (ISMS), a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.
Metadata	Data that describes, or gives meaning to, other data.

DOCUMENT CONTROL

Date	Description	Authors
22/10/18	Annual review 2018 approved by UEB	D. Deighton
10/09/18	Reviewed by Mark Gee, CIO with minor cosmetic amendments and clarifications	M. Gee D. Deighton
20/06/18	Substantially rewritten and expanded to cover both Information Security and Information Management. Reviewed and approved by ISMG.	D. Deighton O. Kew-Fickus
18/09/17	Approved by UEB	D. Deighton
29/06/17	Approved by ISMG with minor changes	D. Deighton
24/03/17	Annual review – amended for overseas campuses, GDPR and some clarification and rationalisation, some paragraph renumbering..	D. Deighton
19/09/16	Annual review 2016 approved by UEB	D. Deighton
07/06/16	Annual review 2016 approved by ISSG	D. Deighton
15/06/15	Annual review 2015 qpproved by UEB	D. Deighton
12/05/15	Annual review 2015 – PCI DSS updates – approved by ISSG	D. Deighton
18/02/14	Annual review 2014 – Asset Disposal, PCI DSS, audit	D. Deighton
23/04/13	Annual review 2013 approved by ISSG	D. Deighton
10/04/12	Revised policy – ISO 27001, NHS IG Toolkit, Data Classification	D. Deighton
29/10/07	Information Security Policy version 0.52	P. Scott