Information Security Policy

1. Introduction

The University has a duty to protect its information assets, ensure business continuity and maximise the flow of information, internally and externally. Information security is vital to ensure effective data sharing, at the same time protecting the information infrastructure from security incidents.

The Birmingham City University Information Security Policy is intended to safeguard the University, University staff, students and owners of intellectual property rights from information security related incidents and any consequential action, loss of income or damage.

The Policy also aims to establish control requirements on network systems, based on the International Standards ISO/IEC 27001 and ISO/IEC 27002.

2. Scope

This Policy applies to all the following groups of staff and students at Birmingham City University.

Anyone accessing **information** that is the property of Birmingham City University

Anyone accessing the Birmingham City University **computer network**

Anyone using **computer equipment** that is the property of Birmingham City University

All Birmingham City University **staff**

All Birmingham City University **students**

Associate **staff** (Visiting Lecturers, KTP Associates)

Visitors to the University who are issued with **temporary guest accounts**

3. Responsibilities

It is the responsibility of all users of University information sources and systems to comply with statutory, University, Faculty and Departmental instructions regarding the safeguarding of information and information media.

It is the responsibility of all users of the University's IT equipment, sources, systems and platforms to comply with the Prevent Duty and the related guidance.

The University will make a summary of this Policy available to all new staff and students at induction and enrolment. The University routinely uses the intranet to make staff aware of the Policy and to inform them of any significant revisions to the Policy.

The University understands its responsibility for managing information correctly. Such information management promotes business efficiency (recognising information as a primary asset, worthy of protection), effective risk management, legal compliance (especially in relation to the General Data Protection Regulation GDPR) and sound corporate governance.

4. Information Security

Information security management has three basic components:

Confidentiality:	Protecting sensitive information from unauthorised disclosure
Integrity:	Safeguarding the accuracy and completeness of information and information processes; practically, this involves identifying key data and rigorously maintaining version control
Availability:	Ensuring that information key to the business of the University is accessible in a timely fashion

5. Access

All staff having access to sensitive data (particularly personal data) are responsible for ensuring that access controls are not compromised by: revealing or allowing access to information by persons not authorised to have it and failing to take reasonable precautions against unauthorised access.

The University provides computer workstations and communications network access to a variety of services hosted either by the University, or by external agencies. Such services shall be used only for work purposes or activities approved by the University.

Access to University information systems is only legitimate if the University has authorised this.

6. Systems Use

All computer systems and network access provided for use by University staff and students are subject to the Conduct and Use of Computer Systems and Networks at Birmingham City University within the Related Policies section of this document.

7. Risk management and information security incidents

All security incidents must be reported to minimise loss and damage to data. Anyone who encounters an information security breach must report it immediately to the IT Help Desk.

Information Technology (IT) will be responsible for giving guidance to the rest of the University regarding a breach, or potential breach of the University's information systems.

With regard to personal data (i.e. data relating to an identifiable living individual) any suspected unauthorised disclosure should be reported to the Data Protection Officer (DPO), responsible for the University's compliance with the General Data Protection Regulation (GDPR).

8. Business continuity

Information security forms part of a wider business continuity context within the University. Information Technology (IT) will ensure all information systems are documented so that should they fail, or if there is a breach from external sources, recovery can be done promptly.

All University information systems are subject to potential loss of data due to failure of hardware or software media. It is the responsibility of Information Technology (IT) (in the case of central systems) and users (for local systems), to regularly make back-up copies of essential data and store it in a safe location, remote from the main system. Computer media should not be carelessly stored.

You can make a request for the backing up of business critical data on central servers at the same time as when you request any new servers or storage arrangements; due to the sizeable overhead associated with data storage, data is not automatically backed up unless you make a formal request.

We will dispose of removable magnetic and optical media containing key business data in a controlled and secure way when it is no longer required, please contact Information Technology (IT) in these instances for advice. We will dispose of redundant computer equipment of in line with the Waste Electrical and Electronic (WEEE) Regulations.

For more information regarding the approach to and the Business Continuity documentation see the links in the Related Policies section of this document.

9. Legal compliance

This Policy is a key component in ensuring compliance with a wide range of legislation governing information. Therefore, the University will try to ensure that its information systems are used within the framework of the law and that the information itself remains lawful.

Section 26(I) of the Counter-Terrorism and Security Act 2015 requires the University to have due regard to the need to prevent people from being drawn into terrorism. In implementing the Duty, the

University will strive to do so in a proportionate manner and to maintain its commitment to the Freedom of Speech (Education Act 1986), the Academic Freedom (Education Reform Act 1988) and the Equality Act 2010.

The General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018 set out the University's legal obligations in relation to personal data; this Policy deals specifically with that principle within it regarding data security. Any particular rules of use of and access to data referred to in this Policy are informed by the Regulation.

10. Consequences of not following this Policy

All users, including any third parties with access to the University's information or computing systems, must comply with the University's *Information Security Policy* as well as all other related Information Technology (IT) policies, including the *Policy for Use of Computer Systems Networks at BCU*. This requirement is included in the *Conditions of Employment* and where appropriate compliance will be monitored.

After investigation if a user is found to have violated the University's Information Security Policy and/or procedures, they may be disciplined in line with the relevant University's disciplinary policy and potentially subject to legal proceedings.

In the case of a student(s) failure to comply with the conditions set out in the University's *Information Security Policy* and *Code of Conduct* this may result in suspension or withdrawal of access to University computer systems and network facilities, and may also render them liable to disciplinary proceedings.

In accepting employment with the University, employees are agreeing that confidential or sensitive documents and data to which they will be given access as part of their duties must be kept confidential. As part of the induction process for new staff, managers must ensure that they draw this to the attention of new staff who will be involved in handling confidential information.

11. Exemptions

Exempt Groups or Individuals
None.

Exempt Equipment
None.

Exempt Circumstances
None.

ANNEX 1: Information to Supplement the Policy

Specific Security Measures

i. The University will provide unique identifiers for every user of the University's information systems
ii. Secure logon procedures and password management systems will be used to access the University's information systems. Passwords: a password is the personal property and responsibility of the individual to whom it is issued; a user must not divulge such password information to any other person unless authorised to do so by the Director of Information Technology (IT). The full User Password Policy is available via this link in the Related Policies section of this document.
iii. Only licensed and authorised software provided by Information Technology (IT) may be used on University System's information.
iv. Computer media must not be carelessly stored in offices. Removable media must be stored discretely in a secure environment where it cannot be obtained by any unauthorised persons.
v. University data classified as legally or contractually restricted must be encrypted.
vi. Staff using any personal data derived from University systems at home must take the appropriate measures to ensure that the data is secure. For instance machines used to access data University information on privately owned computer equipment, whether portable or static, are to be protected by a firewall, operate anti-virus software, and be kept up to date with security patches.
vii. Computer systems and networks which are used to hold personal information and therefore subject to the General Data Protection Regulation (GDPR) should not be created without prior advice from the Data Protection Officer (DPO).
viii. Information Technology (IT) supplies virus protection to the University's information systems.
ix. Where devices, such as laptops, that contain University data are taken offsite (including overseas) appropriate measures must be taken to ensure that data is secure and not accessible. For instance devices must be password protected, be kept up to date with security patches with data encrypted as appropriate. If a device containing University data is lost or stolen, then the IT Help Desk should be contacted as a matter of urgency, so that the network can be protected from the device and to enable it to be remotely wiped where that functionality exists.

IT Systems

All IT purchases should be managed by the Information Technology (IT) department to ensure that software and equipment is fit for purpose, purchased through the correct vendor at the lowest possible price, and the support and on-going costs are fully understood and accounted for.

In some circumstances it is recognised that external services or suppliers will be required for bespoke systems or services by faculties and departments. In this situation Information Technology (IT) will need to be involved; so as to understand and identify where the universities resources are utilised, and the implications on any other services or systems.

The point of contact is your IT Business Partner who will be able to offer advice on the following:

- Impact on other systems or services
- Support costs
- On-going costs
- Details of existing university systems/solutions
- Details of current development and future plans for software and hardware

The IT Business Partners should be involved at the beginning of any faculty or department IT resource planning, system or service purchase.

All users must also be aware of the terms and conditions that they are agreeing to when installing and updating any software for use with university information. Any queries should be directed to the IT Business Partners. Information Technology (IT) is unable to guarantee ongoing support of systems or equipment that has not received their approval before purchase. Information Technology (IT) will not accept any risk or cost implications of systems that are purchased without their consultation.

Physical Access Control

The university access control system is managed by Information (IT) to control who is allowed to enter and use university facilities. The entry system allows staff, students and associates access to the buildings and subsequent restricted rooms on campus via a card entry system.

General Data Protection Regulation (GDPR) and Data Protection Act 2018 Summary

The Data Protection Policy is available via this link.

The General Data Protection Regulation (GDPR) and Data Protection Act impose conditions for the maintenance of personal data in both manual and computer files,this includes data held by staff.. Most of the personal data processed by the University relates to its staff and students. However where necessary the University also processes the personal data of other clients and users of the University's services.

The University is a registered Data Controller under the Regulation. It is an offence to collect, keep, use or disclose personal data in any manner that is not consistent with the University's registration. Staff may use or store personal data derived from the University's systems (e.g. the personal data of students or staff) at home for University purposes only.

It is the responsibility of the creators of any database or manual filing system to ensure that the data held is consistent with the Birmingham City University Data Protection Register entry and in a manner that is consistent with the data protection principles.

Data Protection Principles

As a Data Controller the University must comply with the enforceable principles of good practice. These principles stipulate that the personal data processed by the University must be processed in accordance with the following principles:

1. Lawfulness, fairness and transparency;
2. Purpose limitation;
3. Data minimization; Adequate, relevant and not excessive in relation to the purposes for which they are processed;
4. Accuracy
5. Storage Limitation. Not kept longer than necessary;
6. Integrity and confidentiality
7. Accountability principle

This summary of the data protection principles has been derived from Information Commissioner's website.

Equality Impact Analysis Statement

Birmingham City University's commitment to equality means that this policy has been screened, paying due regard to the general duty in relation to the relevant protected characteristics, the use of comprehensible, inclusive language, and the avoidance of stereotypes. This document is available in alternative formats on request.

Related Policies and Documents

Code of Conduct for Use of Computer Systems and Networks

Data Protection Policy

Staff Password Policy

Student Password Policy

Financial Systems Rules & Training Manuals

University Financial Rules

Identification Card Information

Flexible Working Policy

Information Security Policy Review

This policy will be reviewed on an annual basis, or if there is a change in legal or other business related requirement.

Review Date	Description	Reviewer
10/04/2020	Information Security Policy	IT Security Manager

Document History

Version Date	Description	Authors
25/11/2015	Information Security Policy version 1.4 (Prevent Duty inclusion)	IT Security Manager
22/03/2016	Policy approved and accepted, by University Executive Group (UEG)	UEG approval
03/04/2017	Policy Review – No changes made.	IT Security Manager
02/04/2018	Policy Review – GDPR references added.	IT Security Manager
12/04/2019	Policy Reviewed – GDPR and DPA 2018 references updated	Data Protection Officer