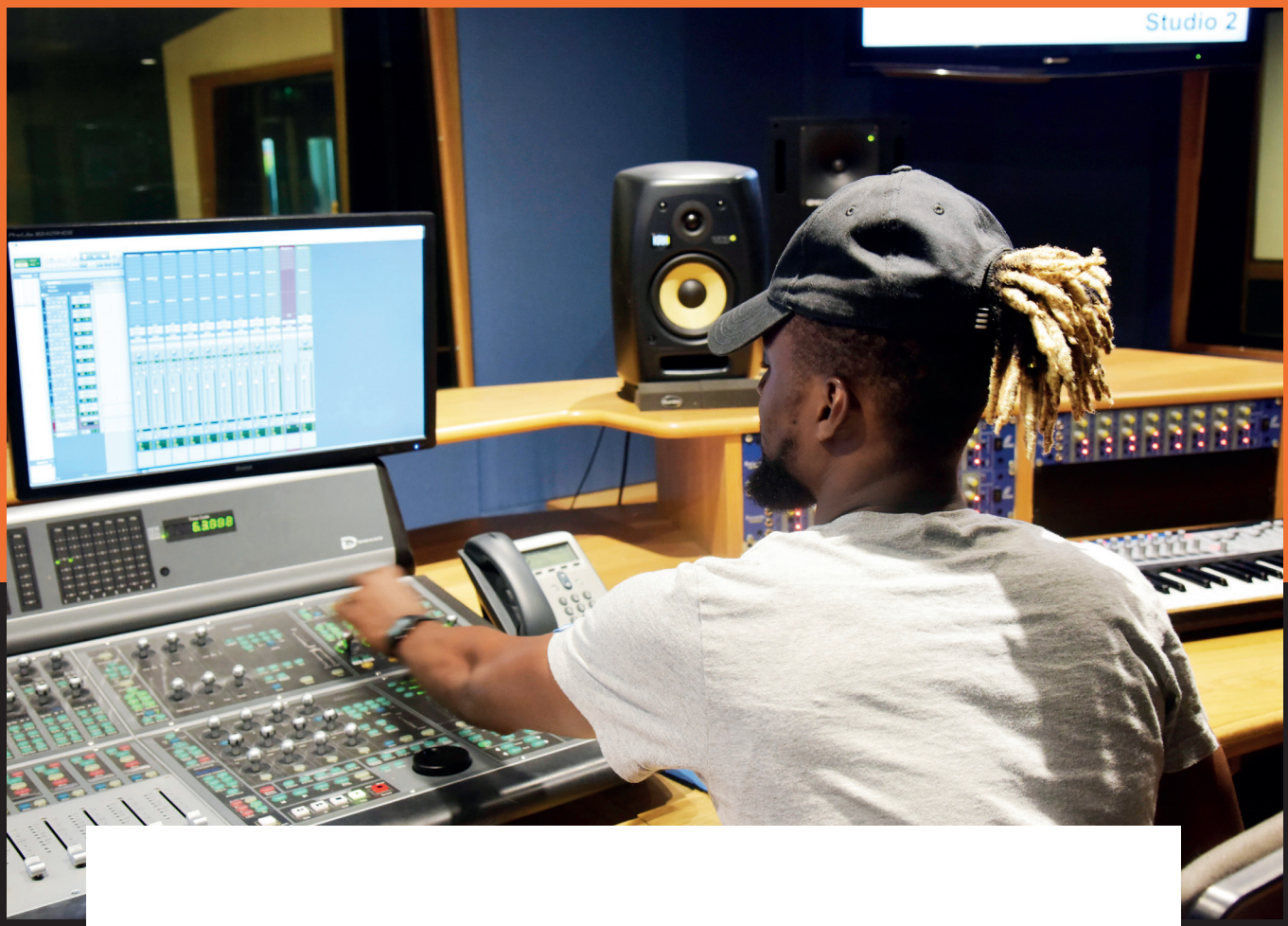
BUCKINGHAMSHIRE
NEW UNIVERSITY
EST. 1891



INFORMATION SECURITY POLICY

bucks.ac.uk

Contents

Purpose Statement	**2**
Applicability and Scope	**2**
Responsibilities	**2**
Assessing the sensitivity of information	**3**
Definitions	**3**
Practical security measures	**4**
Secure storage of data	**4**
Transferring / accessing data securely outside of Bucks New University	**4**
Secure disposal of data	**5**
Data loss and theft	**5**
Practical Support from IS&T Services	**5**

Approved by:	**Operations Board**	Date first published:	**Jun-2015**
Version No.	**1.1**	Date updated:	**Jun-2015**
Owner:	**Information Systems Technology**	Review Date:	**Jun-2016**

This document has been designed to be accessible for readers. However, should you require the document in an alternative format please contact the Academic Quality Directorate.

Purpose Statement

1 Information is a fundamental University asset, required for the effective operation of Bucks New University and the services it offers, including teaching, learning and research; and administrative, management and commercial activities.

2 For the purposes of this policy, information assets include both the electronic data held by Bucks New University and its staff; and the computers, hardware, software and networks used to store and process University data.

3 This policy's objective is to ensure that Bucks New University's information assets are appropriately secured, in order to protect Bucks New University from security incidents that could have an adverse impact on the operations, reputation and professional standards of Bucks New University; or which could result in financial loss. In particular, this policy seeks to ensure legislative compliance and protection against the possible consequences of breaches of confidentiality, loss of Personal Data, failures of integrity or interruptions to the availability of information.

4 This policy should be interpreted in a manner consistent with all other University policies, particularly the Data Protection Policy. It interlinks with a suite of IT policies, the current versions of these policies can be found within the formal documents at Bucks.ac.uk.

Applicability and Scope

5 This policy applies to all:

- information created or received in the course of Bucks New University business and/or entrusted to Bucks New University
- users of Bucks New University information assets, including staff, students, and any other approved users
- locations from which Bucks New University information assets are accessed/used, including all Bucks New University premises, and home or off-site/remote use.

Responsibilities

6 All users of Bucks New University's information assets are responsible for:

- protecting the information assets of Bucks New University and of any third parties to which access is permitted
- compliance with the Data Protection Act 1998, Bucks New University's Data Protection Policy, Bucks New University's Acceptable Use Policy and all other University policies, procedures and guidance relating to security and the protection of information.

7 All staff and students at Bucks New University are responsible for ensuring that the way they handle data on behalf of Bucks New University meets the criteria set out within this policy. Bucks New University welcomes suggestions from staff and students to improve ways in which information is handled.

8 Heads of Department are responsible for ensuring departmental compliance with this policy and shall actively promote compliance to their staff.

Assessing the sensitivity of information

9 The level of security to be applied to information should be proportionate to the nature of the information, its importance and sensitivity. Much of the information within Bucks New University is not confidential and, in many cases, Bucks New University would encourage dissemination of that information as widely as possible. Furthermore, Bucks New University is obliged to publish and/or release on request certain types of data under the Freedom of Information Act 2000. For more information about these obligations, see the FOI section of Bucks New University website. However, it is vital to ensure that confidential information (as defined below) is protected.

Definitions

10 Within this policy the following terms are used:

- **Personal Data**: as defined in section 1 of the Data Protection Act 1998, i.e., information by which a living individual can be identified (directly or indirectly). Examples in a Bucks New University context include: individuals' names, addresses, e-mail addresses, staff/student records, spreadsheets of individuals' details (e.g. assessment records) and information on research subjects. This is not an exhaustive list – see Bucks New University Data Protection Policy for further information.
- **Sensitive Personal Data**: as defined in section 1 of the Data Protection Act 1998, i.e., personal data that relates to a person's racial or ethnic origin, their political opinions or religious beliefs, trade union membership, their state of health, sexual life, or information relating to any offence they may have committed or subsequent proceedings.
- **Commercially Sensitive Information**: information which is not already in the public domain that, if made public, could cause commercial harm to Bucks New University or another party, or which would breach a duty of confidentiality. This is information which may relate to the activities of Bucks New University or its partners, staff and students and which is not intended for general public consumption. Examples could include unpublished information relating to finances, performance, plans and strategies and information relating to contracts, tenders and third party relationships. Commercially Sensitive Information may or may not be exempt from public disclosure under the Freedom of Information Act.
- **Confidential Information**: for the purpose of this document is a catchall referring to information that is either Personal Data and/or Commercially Sensitive Information.
- **Non-Confidential Information**: is already published and in the public domain.
- **Mobile devices**: means any portable device that can store or access data, including laptops, mobile phones, tablets (e.g. iPads) and portable storage devices such as USB pen drives

Practical security measures

11 Protecting Bucks New University's information assets is vitally important to Bucks New University. In order to protect the security of these assets you must:

- Ensure that the use of any IT equipment and systems entrusted to you by Bucks New University is limited to authorised individuals only.
- With the exception of laptops and other mobile devices that are assigned to you, not remove any IT equipment from Bucks New University's premises without the knowledge and approval of either your line manager or the person responsible for the information systems in your department.
- Use passwords only in accordance with Bucks New University best practice guidelines and in particular, never share your password with anybody else.
- Use the appropriate security features recommended by IT Services to ensure that information is protected according to its nature, risk and sensitivity. Contact IT Services for advice as to the security features available and how to access and apply them.
- Use either the 'Lock Computer' or 'Log Off' facilities if you leave your PC desktop or laptop unattended for any period of time. (To do this, press Ctrl-Alt-Del at any time using a Windows device).

Secure storage of data

12 The most secure form of storage for confidential information is Bucks New University's secure, centralised information systems and network drives. Avoid creating unnecessary local copies of confidential Information.

13 If it is absolutely necessary to create or store local copies of confidential information on hard drives or mobile devices:

- Only download and store the minimum amount of information necessary to complete the task.
- External, third party facilities such as cloud storage must not be used to store Personal Data on behalf of Bucks New University and are not recommended for commercially sensitive information.
- The only exception to the above is in circumstances where a third party provider has an agreed, contractual commitment with Bucks New University and will guarantee that the data will be securely held within the EU. (Current examples include Blackboard, Office 365).

Transferring / accessing data securely outside of Bucks New University

14 Confidential information should not be moved outside Bucks New University network or secure information systems unless deemed absolutely necessary. You should first consider whether the data may be accessed via secure login from within Bucks New University's environment or via a secure VPN solution. Consult the IT Service Desk for further guidance.

15 If data transfer is deemed a necessity it should be only the absolute minimum amount of data required and use a level of security appropriate for the nature and sensitivity of the data. Departments may have established procedures for doing this, but if in any doubt, consult the IT Service Desk

16 Where there is a need to share confidential information with external, third parties, such as contractors and suppliers, who are undertaking work on behalf of Bucks New University, a legal agreement may be required to cover data protection and confidentiality obligations. See Data Protection Policy and consult the Data Protection Officer for further guidance.

Secure disposal of data

17 All data must be retained and disposed of in accordance with Bucks New University's Record Management Policy & Retention Schedule.

18 Bucks New University has systems in place for the disposal of confidential waste. IT make the necessary arrangements for securely erasing data and reformatting any IT issued devices before redistributing or disposing of the device as necessary. For more details, see Bucks New University's instructions on waste disposal and recycling.

Data loss and theft

19 Any computer, laptop or other device used to access Bucks New University's network must be kept secure at all times. Please refer to the Mobile Device Security Policy.

20 The loss of any confidential information related to Bucks New University as a consequence of the loss, theft or damage of IT equipment (including both Bucks New University and personal devices) should be reported immediately to the IT Service Desk.

Practical Support from IS&T Services

21 When issuing mobile devices, IT will ensure appropriate security measures are in place to protect Bucks New University's data network and all information systems to minimise the risk of unauthorised access. This includes:

- guidance on alternative technical solutions for the secure transfer of confidential information
- anti-virus software installed, updated and supported on all IT issued devices
- provision and promotion of anti-virus solutions for students' devices
- issuing devices that are configured to be password protected to meet or exceed the standards set out in the Mobile Device Security Policy and Bucks New University's User Authentication & Passphrase Policy
- protecting the Bucks New University network from unauthorised access using lost/stolen devices, by remote wiping the device where that functionality exists.