BISHOP
GROSSETESTE
UNIVERSITY

Document Title:	IT Services – IT Security Policy
Document Category:	Policy
Version Number:	1.1
Status:	Approved
Reason for development:	Change in legislation
Scope:	This policy applies to University staff, students, and authorised consultants
Author / developer:	Head of IT (HoIT)
Owner	Chief Operating Officer
Assessment: (where relevant)	☐ Equality Assessment ☐ Information Governance ☒ Legal ☐ Academic Governance
Consultation: (where relevant)	☐ Staff Trade Unions via HR ☐ Bishop Grosseteste University Students' Union ☒ Any relevant external statutory bodies
Authorised by (Board):	FE&GP
Date first authorised:	20th March 2015
Date current version authorised:	24 February 2021
Date current version effective from:	1 April 2021
Date next review due to commence:	1 April 2022
Document location:	University website
Document dissemination / communications plan	This document will be disseminated to all staff and students within the University via the website
Document control:	All printed versions of the document should be classified as uncontrolled. A controlled version will be available on the [University website / SharePoint].
Alternative format	If you require this document in an alternative format, please contact governance@bishopg.ac.uk

*Please note, this document remains valid until formally revoked or replaced by the University.

IT Security Policy

1 Introduction

1.1 The information managed by the University must be appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information.

1.2 The objectives of this policy are to ensure that:

- all the University's digital services, products, systems, software, and devices are monitored and adequately protected against loss, misuse, or abuse;
- the University is protected from damage or liability resulting from the use of its facilities for purposes contrary to UK law;
- all users are aware of and comply with this policy and supporting documentation;
- prompt action is taken to address security incidents;
- staff are made aware that appropriate security measures must be implemented as part of the effective operation and support of the University's work; and
- all users understand their responsibilities for protecting the confidentiality and integrity of the data they handle.

2 Scope

2.1 This policy is applicable and will be communicated to all staff, students, and other relevant parties. It applies to all digital services, products, devices, and technical infrastructure.

3 Compliance with legislation

3.1 The University must abide by all UK and relevant EU legislation including:

- The Obscene Publications Act 1959
- The Disabilities Discrimination Act 1995 and subsequent amendments to this legislation, for example, the Disabilities Discrimination Act 1995 (Amendment) Regulations 2003
- The Copyright, Designs and Patents Act 1988
- The Computer Misuse Act 1990
- The Data Protection Act 2018
- General Data Protection Regulation (GDPR) 2016
- The Freedom of Information Act 2000
- The Communications Act 2003
- Privacy and Electronic Communications Regulations 2011
- Regulation of Investigatory Powers Act (RIPA) 2000
- Equality Act 2010
- Malicious Communications Act 1988
- Waste Electrical and Electronic Equipment recycling regulations 2013 (WEEE)
- Counterterrorism and Security Act of 2015

3.2 Also, as an organisation authorised to use the JANET communications network, the University must abide by the JANET Acceptable Use Policy.

4 Responsibilities

4.1 Responsibility for ensuring the protection of information systems and ensuring that specific security processes are carried out lies with the Head of Information Technology (HoIT) who is also responsible for the implementation of this policy. The HoIT shall be supported in this by University management and the Chief Operating Officer (COO).

4.3 The HoIT shall provide specialist advice on information security to staff and students when required.

4.2 Third-party users (including agency staff, contractors) of digital services and products are required to agree to respect the confidentiality of any information they encounter during their work/studies and will sign the University's 'External User Agreement Form'. (Available from the IT Helpdesk.)

4.3 This policy shall be reviewed regularly by the HoIT to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies, or contractual obligations.

5 Risk assessment and business impact review

5.1 An IT disaster recovery plan is held within IT Services.

5.2 The *IT Disaster Recovery Plan* should be read in conjunction with the University's *Risk Management Policy* and *Business Continuity (Disaster Recovery) Plan*. It shall be reviewed regularly by the HoIT to ensure that it remains appropriate in the light of any relevant changes to the law, organisational policies, or contractual obligations.

6 Security breaches

6.1 Any user may be held liable for a breach of security.

6.2 IT services shall monitor network activity and take action/make recommendations consistent with maintaining the security of the University's digital services and systems. The HoIT has the authority to take whatever action is deemed necessary to protect the University against breaches of security.

6.3 Any member of staff or student suspecting that there has been, or is likely to be, a breach of security should inform the Information Governance Team immediately by using the data breach form found on the MyDay portal.

6.4 In the event of a suspected or actual breach of security, the HoIT may, normally after consultation with the COO or a member of Vice-Chancellor's Executive Group (VCEG), make inaccessible/remove any unsafe user/login names, data and/or programs on the system from the network.

6.5 Any breach of security of University digital services and systems leading to the loss of personal data is an infringement of Data Protection legislation from 2008 revisions onward and could lead to civil or criminal proceedings. It is vital, therefore, that users of the University digital services and systems comply, not only with this policy but also with the University's *Data Protection Policy*.

7 Precautions in place

7.1 To protect the University against malicious access designed to compromise confidentiality or result in data corruption or denial of service, the University network is protected by a firewall which examines and filters all network traffic into and out of the University. The firewall also acts as a web content filtering system to prevent access to inappropriate internet material.

7.2 All e-mail communications, those received from external sources as well as those generated internally, and including attachments, are automatically checked for viruses by networked anti-virus and anti-spam software before being opened by the intended recipient(s).

7.3 All staff e-mails, to and from mailboxes, are automatically archived to a dedicated server for five years to ensure data compliance.

7.4 All network files are automatically scanned for viruses once a day.

7.5 Unsolicited mail presents a security (virus) threat to the University. Any such emails which lack obvious signs of business relevance will be returned to the sender and the intended recipient (if identifiable) will be notified that this action has occurred. If the sender persists in sending such emails the HoIT will notify the System Administrator at the sender's source.

8 Data Security

8.1 The University holds a variety of sensitive data including personal information about applicants, students, and staff. If you have been given access to this information, you are responsible to contextually comply with GDPR and relevant data protection legislation and guidance.

8.2 There are a variety of methods of remote access to digital services and systems available (in particular, virtual desktop, VPN and Microsoft 365) which allow you to work on data in-situ rather than taking it outside the University and these should **always** be used in preference to taking data off-site.

8.3 You should only take a copy of data outside the University's services if necessary, and you should exhaust all other options before doing so. This includes putting sensitive data onto portable media devices, laptops, smartphones, tablets, your own device (BYOD), CDs/DVDs or into emails etc. If you are in doubt as to whether data can be taken outside the University you are required to err on the side of caution, consult your line manager, information governance, or seek advice from the IT Services Helpdesk.

8.4 To help maintain your cybersecurity in-line with industry best practice your BGU IT user account password expires every 90 days for staff/consultants and 180 days for students.

9 Laptop Security

9.1 All University laptops and similar devices must be encrypted to at least the required University specification; IT Services do this on your behalf by enabling Bit locker.

9.2 All laptops must always be kept secure by the employee responsible for them. When unattended, laptops must always be kept in a locked area (e.g., a locked room or cabinet).

10 Portable Media Security

10.1 Portable Media by definition are readily transportable items used to store information in digital form (whether temporarily or long-term), including USB memory sticks ("flash drives"), memory cards, smartphones, compact discs (CDs and DVDs), plug-in external drives, and media players (mp3 players).

10.2 No personal or confidential information shall be stored on any non-University portable media except as explicitly provided for in contracts with third parties providing goods or services to the University.

10.3 No personal or confidential information shall be stored on any portable media unless the storage media is encrypted to the required University specification and approval has been granted by your line manager in line with GDPR compliance and data protection regulations. It is your responsibility to ensure this is in place.

10.4 Encrypted portable media, when not in use should be kept securely locked away.

11 Tablet & Smartphone Security

11.1 If you use a University-owned tablet/smartphone or using your own devices to access University digital services and systems, you must comply with this policy and the BYOD policy.

If you are uncertain about any aspect of data security, you must contact the IT Helpdesk for advice.

12 Compliance and current awareness

12.1 Failure of an individual student or member of staff to comply with this policy may lead to the instigation of disciplinary proceedings and, in certain circumstances, legal action. Failure of an agency worker or contractor to comply could lead to the cancellation of a contract.

12.2 University staff and students by using their University IT user account are automatically accepting the terms of this policy and the *IT Systems Acceptable Use Policy*.

12.3 The University shall establish and maintain appropriate contacts with other organisations, regulatory bodies in respect to its information security policy.

13 Linked documentation

Data Protection Policy

IT Disaster Recovery Plan

Risk Management Policy

Business Continuity (Disaster Recovery) Plan.

IT Acceptable Use Policy

Computer Equipment Disposal Policy

Electronic mail Interception Policy

IT Services - Bring Your Own Device (BYOD) Policy

External User Agreement Form

14 Security of premises

14.1 While it is difficult to make premises in a University environment completely secure, most buildings and offices are now equipped with either key or keypad locks which provide a reasonable level of protection against opportunist intruders, so long as they are used properly by those who have a right of access.

14.2 To reduce the risk of theft, the following rules should be observed:

- Offices or other rooms which house valuable equipment should not be left unattended with the door unlocked or (on the ground floor) with windows open.

- When entering a locked building the door should be closed securely behind you and you should not allow access to anyone who tries to ‘tail-gate’ behind you.
- Report any suspicious behaviour to the Security Office.
- Where buildings/offices are secured by card-controlled doors or keypad locks, do not lend your card to anyone, or give away details of PIN/keypad numbers.
- Valuable equipment or equipment storing valuable data should not be in a vulnerable location such as just inside the window of a ground floor office or near a fire escape; curtains and blinds should be closed at night and equipment which can be seen from the outside should be covered if possible.

15 Security of equipment

15.1 The HoIT and the HoIS maintains a detailed inventory of all key IT equipment, including servers, gateways, UPSs, workstations, specialised equipment, and back-up media. The inventory includes information on the model and serial numbers, BG security markers, locations, and usage details. All computers are security marked and their details recorded by the HoIT and HoIS on a departmental inventory. This is done as soon as possible after the installation and set-up of the equipment.

15.2 To ensure your computing equipment is secure:

- If appropriate, carry out a risk assessment to determine if any additional security measures need to be taken (cable restraints, lock-down fixtures, alarms).
- Dispose of any computer packaging as quickly and as discretely as possible in order not to advertise the arrival of new equipment.
- Do not re-locate IT equipment or services without contacting the IT Helpdesk.

16 The security of data

16.1 Departments holding data which is backed-up should ensure that the back-up data is held securely (e.g., in a locked fire-proof container or cupboard) and placed in a location commensurate with the department’s procedures for ensuring business continuity. i.e., away from the area where that data is normally processed. This should be done in liaison with the HoIT or HoIS.

16.2 For guidance on data protection please refer to the University’s *Data Protection Policy*.

16.3 If you need to dispose of IT equipment, please contact the IT Helpdesk. We will ensure that any data held on the equipment is securely destroyed in accordance with the Data Retention Schedule by an approved method and the equipment is recycled in line with the Waste Electrical and electronic equipment recycling regulations (WEEE).

16.4 Encrypting Devices: Encryption is a means of preventing anyone other than those who have a key from accessing data, be it in an email, on a computer or a storage device. In all cases, you need to consider the security of the encryption key(s) and it is recommended that you lodge these securely with a trusted third party (who, preferably does not have access to the files) to ensure their availability in the event of key loss.

17 The reporting of security incidents

17.1 It is essential that incidents affecting the security of the Universities information systems, or with the potential to do so, should be **reported immediately** to the IT Helpdesk. Following this, the HoIT, HoIS or COO who will take whatever immediate action is considered necessary.

17.2 Users of the Universities digital services and systems should report any observed or suspected security vulnerabilities or concerns to the IT Helpdesk.

17.3 Where the software does not appear to be working correctly, the matter should be reported to the IT Helpdesk. If it is suspected that the malfunction is due to a malicious piece of software e.g., a computer virus, they should stop using the computer, note the symptoms and any messages appearing on the screen and report the matter immediately to the IT Helpdesk.

17.4 Where incidents take the form of misuse of a digital service or system, or data contained thereon, the HoIT or HoIS will normally suspend the user account pending further investigation and advise the COO or a member of VCEG.

17.5 The HoIS will keep a log of security incidents so that the effectiveness of the implementation of the Information Services Security Policy can be monitored.

18 Virus protection

18.1 A virus is a piece of software deliberately designed to distribute itself from one computer system to another without the knowledge of the user. Viruses can spread rapidly causing disruption and damage.

18.2 Endpoint protection software is installed on University owned devices.

18.3 If any BGU service is affected by a virus, affected service users will be notified directly.

18.4 If you suspect that your device has been infected with a virus you should turn the device off and contact the IT Helpdesk.

19 The wireless network

19.1 Bishop Grosseteste University provides a wireless network across our campus. To access the wireless network, devices are recommended to have up-to-date anti-virus software and up-to-date software.

19.2 Users of the wireless network are required to adhere to the *IT Systems Acceptable Use Policy* and the *Wireless Network Guidelines.*

19.3 To limit the potential security risks that may be associated with wireless network technologies, access to the wireless network must take place in a controlled and secure manner. To this end, use of the wireless network is monitored by IT Services.

20 Using Tablets and Smartphones

20.1 If you are considering purchasing a Tablet or Smartphone please contact IT Services who will advise on the purchase of a compatible device for University use.

20.2 IT Services can assist users to connect their own devices to the Universities wireless networks. The assistance will include the initial synchronisation of the device to BG Email systems. Please refer to the Bring Your Own Device (BYOD) Policy.