BISHOP GROSSETESTE UNIVERSITY

Document Title:	IT Systems Security Policy
Document Category:	Policy
Version Number:	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 Infrastructure & Support
Owner	Director of IT
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):	SLT
Date Authorised:	20th March 2015
Effective from:	21st March 2015
Review due:	20th May 2019
Document location:	University website
Document dissemination / communications plan	This document will be disseminated to all staff and students within the University via the Corporate Leadership Team
Document control:	All printed versions of the document should be classified as uncontrolled. A controlled version will be available on the [University website / Staff Portal].

IT Systems Security Policy

1 Introduction

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.

The objectives of this policy are to ensure that:

- all of the University's IT systems, software and equipment 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 fully 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;
- all users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle.

2 Scope

This policy is applicable and will be communicated to staff, students and other relevant parties. It applies to the University College network in its entirety and all non-networked departmental systems and PCs.

3 Compliance with legislation

The University College has an obligation to 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 1998
- The Freedom of Information Act 2000
- The Communications Act 2003
- Privacy and Electronic Communications Regulations 2011
- Regulation of Investigatory Powers Act (RIPA) 2000
- Copyright, Designs and Patents Act 1988
- Equality Act 2010

- Malicious Communications Act 1988
- Counter-Terrorism and Security Act 2015

In addition, as an organization authorized to use the JANET communications network, the University College has an obligation to 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 Director of IT (DoIT) who is also responsible for the implementation of this policy. The Director of IT shall be supported in this by University management and in particular by the Director of Resources (DoR).

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

4.2 Third party users (including agency staff, contractors) of IT systems are required to agree to respect the confidentiality of any information they encounter in the course of their work/studies.

4.3 This policy shall be reviewed regularly by the Director of IT 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 Risk assessments and business impact reviews for IT systems are contained with the *IT Systems Disaster Recovery Policy*.

5.2 The IT Systems Disaster Recovery Policy should be read in conjunction the University's *Risk Management Policy* and *Business Continuity (Disaster Recovery) Plan*. It shall be reviewed regularly by the Director of IT 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 in security.

6.2 The Director of IT shall monitor network activity and take action/make recommendations consistent with maintaining the security of University IT Systems. The Director of IT 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 IS security should inform the Director of IT immediately.

6.4 In the event of a suspected or actual breach of security, the Director of IT may, normally after consultation with the Director of Resources or a member of the SLT, 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 IT systems leading to the loss of personal data is an infringement of the Data Protection Act 1998 and could lead to civil or criminal proceedings. It is vital, therefore, that users of the University College information systems comply, not only with this policy, but also with the University's Data Protection Policy.

7 Precautions in place

7.1 To protect it 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 a period of 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 Director of IT will notify the System Administrator at the sender's source.

8. Data Security

The University holds a variety of sensitive data including personal information about students and staff. If you have been given access to this information, you are reminded of your responsibilities under data protection law.

You should only take a copy of data outside the University's systems if absolutely necessary, and you should exhaust all other options before doing so. This includes putting sensitive data onto laptops, memory sticks, cds/DVDs or into emails. If you do need to take data outside the University, this should only be with the authorisation of your Head of Department and a record logged. As part of this you should perform a risk assessment on the implications of it falling into the wrong hands, and take appropriate steps to mitigate against this. This will almost certainly include **encrypting** the information, and checking the data protection statements of any recipients of the data.

There are a variety of methods of remote access to systems available (in particular, VMware Horizon View and SSL VPN) 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.

IT Services offers a variety of information and support to help you keep data secure.

Laptop Security

All University laptops and similar devices must be encrypted to at least the required University specification; IT Services recommend that users use Truecrypt software or if you are using Windows 7 Enterprise, IT Services recommend Bit-locker.

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

Portable Media Security

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

No personal or confidential information shall be stored on any portable medium unless at least one of the following conditions is met:

1. The storage medium is encrypted to at least the required University specification
2. Unencrypted portable media are used only in a single location and are kept securely locked away at all times when not in use.

Note that, owing to the risk of user error, we do not recommend the use of an unencrypted storage medium where confidential or personal information is stored in encrypted folders or files.

Tablet & Smartphone Security

If you use a University-owned tablet/smartphone or using your own personal devices to access University information systems, you must comply with this policy.

This policy necessitates a complex password of at least eight characters. Users should ensure that they turn Passcode On and Set Simple Passcode to OFF.

Using Auto-Lock will prevent unauthorized users from accessing your tablet/smartphone if it is left unattended after a specific time period; it is recommended that this time period is no longer than 5 minutes.

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

9 Compliance and current awareness

9.1 This policy shall be made available to all members of staff and students via the University website.

9.2 Authorised third parties and contractors given access to the University network shall be advised by the Director of IT or Head of Infrastructure and Systems (HoIS) of the existence of this policy.

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

9.4 University staff and students shall be made aware of the IT Systems Acceptable Use Policy at induction.

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

9.10 This policy also conforms to the guidelines of the Prevent agenda

10 Linked documentation

IT Systems Security: Notes of Guidance

Password Policy

Data Protection Policy

IT Systems Disaster Recovery Policy

Risk Management Policy

Business Continuity (Disaster Recovery) Plan.

IT Acceptable Use Policy

Computer Equipment Disposal Policy

Electronic mail Interception Policy

11 Appendices

Notes of Guidance

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.

12 Security of premises

12.1 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.

12.2 In order 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 Porters;
- 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 located 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.

13 Security of equipment

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

13.2 In order 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 move IT equipment or other IT facilities without first checking with the DOIT or HoIS.

14 The security of data

14.1 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 DoIT or HoIS.

14.2 For guidance on data protection please refer to the Universities Data Protection Policy.

14.3 Before disposing of computing equipment staff should ensure that any data held on the hard disk is destroyed by an approved method. Please refer to the Computer Equipment Disposal Policy or seek advice from the DoIT or HoIS if necessary.

14.4 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 on a storage device. In all cases you need to consider the security of the encryption key(s) and it is recommend that you lodge these securely with a trusted third party (who, preferably doesn't have access to the files) so as to ensure their availability in the event of key loss.

15 The reporting of security incidents

15.1 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 DOIT, HoIS or the Director of Resources (DOR) who will take whatever immediate action is considered necessary.

15.2 Users of the Universities IT systems should report any observed or suspected security weaknesses in or threats to those systems to the DoIT, HoIS or the DOR.

15.3 Where software does not appear to be working correctly, the matter should be reported to the IT Helpdesk or the HoIS if the implications of the fault are severe. 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 or HoIS.

15.4 Where incidents take the form of misuse of a system, or data contained thereon, the DoIT or HoIS will normally suspend the user account pending further investigation and advise the DOR or a member of the Senior Leadership Team.

15.5 The HoIS will keep a log of security incidents in order that the effectiveness of the implementation of the Information Systems Security Policy can be monitored.

16 Virus protection

16.1 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 cab spread rapidly causing disruption and damage.

16.2 As a precaution, anti-virus protection software is installed on the University network. Virus scanners however are not fool proof and are largely reactive to new viruses leaving a window of opportunity for new viruses before being detected and incorporated into a scanner.

17.3 In the event that any BG system is affected by a virus, users will be notified via e-mail and / or the BG website.

18.4 In order to protect your computer from virus infection:

- Do not open e-mails (and especially attachments) if you do not know their origin;
- Make sure that your e-mail client e.g. Outlook does not automatically open attachments when reading e-mails;
- Always scan media (i.e. CDs, USB drives). To do this, insert the media into your PC, open up *My Computer*, then right click on that drive and choose *Scan with Sophos Antivirus*.
- If you lend an external device (e.g. a memory stick and hard drive) to someone, always scan it when it is returned;

18.5 If you suspect that your computer has been infected with a virus you should:

- Stop sending emails immediately;
- Take the computer off the network by physically removing the network cable;
- Contact the IT Services department and not use the computer again until they say so.

IT Services will attempt to isolate the infected computer, research the virus, remove the virus, check other PCs/servers and try to find out how the virus was transmitted.

18.6 Macro viruses use an application's own built-in macro programming language to distribute themselves and corrupt documents. By enabling Word's *Macro Virus Protection* tool you will be prompted if there is a macro in the document you are about to open. If you suspect that the macro may be infected with virus it is possible to disable the macro and continue to open the document:

- On the Word menu bar go to Tools →Options→General;
- Check the box labelled *Macro Virus Protection.*

Excel documents can be similarly protected.

19. The wireless network

19.1 Bishop Grosseteste University provides a wireless computer network to selected areas of the campus. To access the wireless network computers and laptops must be running up-to-date anti-virus software and an up-to-date personal firewall. Resident students who use their own computers/laptops and do not currently have anti-virus software and/or a personal firewall the University will provided with them by the University.

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 In order 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.

In order to manage and monitor the wireless network, and to identify rogue devices and possible misuse of the network, IT Services will make periodic sweeps of the wireless network coverage areas.

20 Using Internet Tablets and Smartphones

20.1 If you are considering purchasing an Internet Tablet or Smart phones 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 devices to the Universities wireless networks. The assistance will include the initial synchronisation of the device to BG Email systems

Security of Tablets and Smartphones:

20.3 Do power your mobile device down fully so that if it is stolen, the data cannot be accessed.

20.4 Do keep the phone numbers of the people you work with most closely.

20.5 Do delete phone numbers when they are no longer required for work purposes.

20.6 Do have a securely held backup of data in the event of the encrypted item being lost or stolen or of forgetting the encryption key

20.7 Don't leave tablets or phones unattended

20.8 Don't store or process restricted University data or personal data on a non-encrypted mobile or storage device.

20.9 Don't simply put your encrypted mobile device into sleep mode when it is at risk of theft (e.g. whilst in transit).

20.10 Don't copy the entire University contact directory to your mobile phone.