BISHOP GROSSETESTE UNIVERSITY

Document Title:	IT Systems: Acceptable Use 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 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 March 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: Acceptable Use Policy

This policy is for the benefit of all users of University IT systems and can be enforced by any member of staff. It concerns the use of University IT systems including hardware & software, and networked, stand-alone, hard-wired and wireless equipment. New students and staff should be made aware of this policy at induction.

1. Use of University IT systems

1.1 University IT systems are primarily for academic, administrative or other authorised use.

2 Acceptable use of University IT systems

2.1 Users must comply with all statutory policies and rules in force and applicable to IT facilities provided by the University and third parties, including the Data Protection Act 1998; Obscene Publications Act 1959; Computer Misuse Act 1990; Copyright, Design and Patents Act 1988; Regulation of Investigatory Powers Act 2000; Freedom of Information Act 2000; Communications Act 2003.

2.2 Users are responsible for the security of their own user accounts. Passwords must not be released to anyone else. Change your password if you think it has been compromised.
It should be borne in mind that giving your user id and password for your University system to a friend or acquaintance, who is not an authorised user, could result in a court appearance, should a complaint be made to the police by the University.

2.3 Do NOT leave a PC or Virtual Terminal logged into your account and unattended – users are to log out or lock to PC/Virtual Terminal when you have finished.

2.4 Users are required to check their University e-mail accounts regularly.

2.5 All data should be stored either in the users' H:\ drives, Sharepoint or the BGU OneDrive. Data stored elsewhere is subject to removal without notice. Please note: BGU reserves the right to access H:\ drives, Sharepoint or BGU OneDrive in the interests of business continuity and security. All access will be approved by either the Head of HR or the VC.

2.6 Users must comply with the licence agreements for software programs held by the University (the illegal copying of licensed software can incur civil damages and/or criminal penalties).

2.7 Users must comply with the JANET Acceptable Use Policy which is available to view at janet.ac.uk

2.8 Material published on the University SharePoint, Website or VLE must conform to the University's policies, procedures and copyright licences. Such material must not risk criminal prosecution or civil legal action or be inappropriate for publication by the University.

3 Misuse of University IT systems

3.1 The misuse of IT systems threatens the security of the University. Misuse applies to the transmission of information be it personal or University-related. The University recognises three levels of misuse: general misuse, serious misuse and criminal misuse.

3.1.1 **Examples of general misuse:**

- Disclosing a network username and password to another person;
- Sending repeated and/or unsolicited network or other emails, particularly if they are not University-related;
- Sending e-mails using an alias, pretending to be someone else, or using someone else's e-mail account without their permission;
- Downloading material which could be harmful to the integrity of the University's systems. This may be considered serious misuse in an instance where a warning about a virus or similar threat issued by the University is subsequently ignored.

3.1.2 **Serious misuse** implies intent to harm. Violations such as these almost certainly imply the initiation of University disciplinary processes and/or legal proceedings. Examples of serious misuse are:

- Viewing, printing, storing, displaying or electronically distributing inappropriate material or material which may be considered offensive to others;
- Attempting to gain unauthorised access to a computer or restricted areas of the University Network
- Copying, modifying, disseminating or using electronic information belonging to another user without the permission of the owner;
- Access or try to access data which he or she knows or ought to know is confidential
- Intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software
- Introduce packet-sniffing or password-detecting software
- Carry out any hacking activities
- Transferring copyrighted software from the network to a private computer, and
- Uploading program files, MP3 files or other copyrighted material from a personal computer located on or off campus, to personal network space on the University network.
- Damaging or tampering with computing equipment
- Sending e-mails or posting material from a University computer onto an internal or external bulletin board, social media resource or website of a threatening, discriminatory or obscene nature or which may be considered to be slanderous or libellous or which directly or by association bring the University into disrepute;
- Using a computer connected to the University network to publish material forbidden by UK/EU law, or to store material of a criminal nature;
- Preventing bona fide students/staff from accessing computing resources, e.g. by removing hardware;

- Altering data without authorisation or destroying data held on the network;
- Storing, processing or electronically distributing personal data contrary to the University's notification under the Data Protection Act 1998.

3.1.3 **Criminal misuse** implies very serious violations necessitating legal proceedings. Serious misuse can become criminal misuse if the scale is of sufficient magnitude. In this event the University may be obliged to call in the Police. Criminal misuse includes the illegal copying of licensed software.

4 Personal or commercial use of University IT systems

4.1 Limited, non-profit (non-commercial) private/personal use of University internal IT systems is permitted if such use does not disrupt or distract the individual from the conduct of University business or restrict the use of those systems by other legitimate users.

4.2 Any use of University IT facilities for personal/private use which might incur a financial charge upon the University is expressly forbidden. Personal use of the University's IT facilities must comply with all relevant University polices and external laws, including the Data Protection Act 1998.

4.3 The use of University IT facilities for commercial gain by an individual or group must have the explicit permission of the Vice Chanceller. Such permission may be withdrawn at any time for any reason.

4.4 University laptops and netbooks should not be used for personal home use and software not registered with the University should not be installed without prior permission from the Head of IT or the IT Operations Manager.

4.5 Individuals must seek permission from the Head of IT before connecting any personal home PC/Laptop to the corporate LAN (this does not apply to the wireless network). IT Services may disconnect any unauthorised host from the network without warning.

5 Electronic mail

5.1 The University e-mail system is the accepted and official means of e-mail communication between members of the University community, providing equitable and reciprocal e-mail access to all departments, members of staff, and students. E-mails from members of staff and students about University business should only be sent to and from University e-mail accounts. Members of staff and students are requested to check their University e-mail accounts on a regular basis to ensure that the system works effectively for all users.

5.2 Group e-mails are messages sent from one person to a group of people. Examples of groups include all of the students on a particular course, the members of a Students' Union society, or all of the students at the University. Students and members of staff should expect to be sent group e-mails about University-related matters. These may include e-mails from the Students' Union.

5.3 Group e-mails, and particularly those sent to 'all students' or 'all staff' should only be sent if the contents are appropriate to a *significant* majority of the recipients and are University-related. Care should be taken to be concise, polite and courteous, and attentive to spelling and grammar.

5.4 The attaching of files to large group e-mails ('all staff' or 'all students') should be avoided. Instead, files should be made available on the University VLE or website or in a public e-mail folder.

5.5 BGU may under permitted circumstances authorise access to an individuals mailbox, further information can be found within the Electronic Mail Interception Policy.

5.6 Generic email aliases must be specific to the faculty/department. Generic emails such as info@bishopg.ac.uk shall not be given to an individual school or department unless there is no possibility of the word being needed by any other School or department in the future. In addition, thought should be given when devising the email address so that it is easy for the end-user to remember and type accurately.

5.7 In all cases any requests for generic email addresses must be submitted to Marketing who have to approve their creation before any literature or advertising is commissioned.

5.8 Details of the generic email address should be forwarded to the IT Help Desk so that it can be included in the email address directory and, where it is to be used for promotion, a generic email address should always be used in preference to a personal one.

5.9 Generic email addresses should be accessible to at least two members of staff; individuals will not be allocated a generic address. This helps to guarantee a prompt and effective response. Any changes to users of the email address, including when applicable staff leave, should be reported to the IT Help Desk so that the information relating to the email address can be updated.

6. Monitoring of Electronic Communications

BGU reserves the right, without notice, to access, listen to or read any communication made or received by you on our computers for the following purposes:

- to establish the existence of facts
- to ascertain compliance with regulatory or self regulatory practices and procedures
- for quality control and staff training purposes
- to prevent or detect crime (including 'hacking')
- to intercept for operational purposes, such as protecting against viruses and making routine interceptions such as forwarding e-mails to correct destinations
- to check voice-mail systems when you are on holiday or on sick leave.

We reserve the right to monitor time spent by users accessing the Internet for browsing. We may monitor sites visited, the content viewed or information downloaded where necessary.

We reserve the right to make and keep copies of e-mails and data documenting use of the e-mail and/or the Internet systems, for the purposes set out above. We may bypass any password you set.

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

7. The wireless network

7.1 In addition to the examples of misuse outlined in section 3 above, the following examples of misuse apply specifically to the University's wireless network:

- configuring wireless cards in 'ad hoc' mode (which allows one user to access another user's mobile device e.g. for gaming purposes);
- running peer-to-peer (P2P) file sharing software, e.g. Kazaa;
- intercepting or attempting to intercept other wireless transmissions for the purposes of eavesdropping;
- accessing or running utilities or services which might negatively impact on the overall performance of the network or deny access to the network, e.g. radio-frequency jamming, denial of service;
- provide services which may interfere with normal network operation.

8 Smart phones

8.1 Smart phones should be stored securely when not in use and be password-protected. Staff should not download confidential University files onto a smart phone without encrypting the data.

9 Disclaimer

9.1 Whilst the University takes appropriate security measures against unauthorised access to, alteration, disclosure, destruction or accidental loss of personal and other data it cannot and does not give any warranties or undertakings to users about security, confidentiality or integrity of data, personal or other.

9.2 Other than any statutory obligation, the University will not be liable for any loss, damage or inconvenience arising directly or indirectly from the use of, or prevention of use of, any IT facility provided and/or managed by the University.

9.3 The University is not responsible for material accessed off campus via the internet.

10. Breaches of this policy

10.1 Any suspected breach of this policy should be reported to a member of the IT Services team. The matter will then be investigated. The University reserves the right to suspend user accounts pending the investigation of suspected breaches of policy.

10.2 Data/programs created/owned/stored by users on or connected to University IT facilities may in the instance of suspected wrong-doing, be subjected to inspection by the Head of IT, a member of the SLT or other authorised person.

10.3 Should the data/programs be encrypted the user shall be required to provide the decryption key to facilitate decryption of the data/programs. Where evidence is found of misuse or of the illegal use of material the material will be subject to removal/deletion.

11 Linked documentation

IT Systems Security Policy
IT Systems Security Guidelines
Password Policy
Data Protection Policy
Wireless Network Guidelines