Brunel IS Acceptable Use Policy (BACUP)

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security officer

Document History

Version	Author	Comments	Date
V 1.0	Andrew Clarke	Initial Draft	27/03/2018
V 1.1	Andrew Clarke	Format Changes – Strategy & Governance	03/05/2018
V 1.2	Andrew Clarke	Repetitions removed, distinction made between private office areas and public spaces, behavioural change to remove mobile use, ID badge wear removed, and personal use redefined as staff personal use	18/07/2018
V 1.3	Andrew Clarke	Grammar + Syntax amendments - Head of Infrastructure and Operations	31/07/2018
V 1.4	Andrew Clarke	CISA Approval (added must be read in conjunction with the BACUP (IS Acceptable Use Policy)	07/09/2018
V 1.5	Andrew Clarke	InfoSub Committee – Dr Stephen Swift exceptions for legitimate research and teaching that may require provisional exemptions from some policy controls guidelines (p7 and p10) Software installation clarification on managed builds. (p.20)	12/02/2019
	Andrew Clarke	Annual Review	08/06/2020

Document Approval

The contents of this document are classified as Protect to Brunel University London (BUL) information classification. Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.

This document requires the approval from BUL as defined in the ISMS Compliance document.

Owner: Michael Jenkins	Chief Information Security Officer
Signature: MGJ	Date: 07 Sep 2018
Approver: Pekka Kahkipuro	Chief Information Officer
Signature: PK	Date: 07 Sep 2018
Distribution:	

Contents

1.	About this document	4
1.1	Purpose	4
1.2	Responsibilities	4
1.3	ISO27001 Conformance	4
1.4	Scope	4
1.5	References	5
1.6	Principles	5
2.0	Acceptable Use Policy	7
2.1	Policy Framework	7
2.2	Exceptions process	8
2.3	Policy Compliance	8
3.0	Network IS	10
4.0	Email and Communication Activities	12
5.0	Monitoring	12
6.0	Harassment	14
7.0	Defamation	14
8.0	Social Media / Blogging	15
9.0	Printing	15
10.0	Passwords	15
11.0	Classification - University Confidential and Protect information	15
12.0	Incidents and Damage	16
13.0	Offensive material	17
14.0	Remote access	17
15.0	Physical security	17
16.0	Data Protection	18
17.0	Logs information	19
18.0	Legislative and Copyright	19
19.0	Reputational damage	19
20.0	Staff Personal use	19
21.0	Software & Mobile Apps	20
22.0	Behaviour	21

1. About this document

1.1 Purpose of Document

The purpose of this policy is to outline the acceptable use of IT equipment at Brunel University London. These rules are in place to protect the employee and Brunel University London. Inappropriate use exposes the University to risks including virus attacks, compromise of network systems and services, data breaches and legal situations.

This policy must be read in conjunction with the BACUP (IS Acceptable Use Policy)

Please refer to Brunel University London ISMS Document *BUL-GLOS-000 - SyOPs Glossary of Terms* for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

1.2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
Cyber & Information Security Manager	Is responsible for maintaining the acceptable use policy and to ensure that the Policy continues best practice and ensuring compliance with legislative and regulatory requirements.
All Users	It is the responsibility of all users of Brunel University London's IS services to read and understand this policy. This policy may be updated from time to time, in order to comply with legal and policy requirements.

1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A8 – Asset Management
ISO 27001:2013 Conformance Control	Information Classification Objective A.8.1.3 Acceptable use of assets

1.4 Scope

This policy applies to employees, contractors, consultants, temporaries, other workers, students and affiliates at Brunel University London, including all personnel affiliated with third parties.

This policy applies to all equipment that is owned or leased by Brunel University London and to the use of information, electronic and computing devices and network resources to conduct Brunel University London business or interact with internal networks and university systems,

whether owned or leased by Brunel University London, the employee, or a third party. It also extends to information held on behalf of third parties and partners.

This policy also applies when using your own device to store, access or process information on Brunel University London Information Systems.

This policy applies at all times when using Brunel University London information Systems and not just during your normal working hours.

All employees, contractors, consultants, temporaries, other workers, students and affiliates at Brunel University London and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Brunel University London policies and standards, and local laws and regulation.

Brunel University London seeks to promote and facilitate the positive and extensive use of IT in the interests of supporting the delivery of learning, teaching, innovation and research to the highest possible standards. This also requires appropriate and legal use of the technologies and facilities made available to students, staff and partners of the University.

This Acceptable Use Policy is taken to include the JISC Acceptable Use Policy and the JISC Security Policy published by JISC (UK), the Combined Higher Education Software Team (CHEST) User Obligations, together with its associated Copyright Acknowledgement, and the Eduserv General Terms of Service. The University also has a statutory duty, under Section 26 of the Counter Terrorism and Security Act 2015, termed “PREVENT”. The purpose of this duty is to aid the process of preventing people being drawn into terrorism.

1.5 References

- BACUP (IS Acceptable Use Policy)
- BUL-POL-08-02 Information Classification
- BUL-POL-9.4.3 - Password Policy
- JISC Acceptable Use Policy
- BUL-POL-EMAIL - Email Use Policy
- BUL-POL-LEGIS - Legislative and Regulatory Framework Policy
- BUL-POL-SOCIAL- Social Media Use Policy
- BUL-POL-6.1.2 - ISMS Asset owners Roles and Responsibilities

1.6 Principles

The security of Brunel University London’s data network against unauthorised use and access must be a primary concern of each and every user at all times. It is a clear breach of this Policy to act with disregard, whether wilful or negligent, for best practices of information security, and such disregard may lead to the institution of disciplinary proceedings against any transgressor.
The connection of devices to the data network of Brunel University London must always be made in accordance with the current rules of Information Services. These rules cover, but are not limited to, the acceptable level of protection against viruses, worms and other malware. It is the user’s responsibility to confirm current requirements before attempting to connect any machine which does not enjoy the University’s standard PC image (whether

that machine is Brunel University London property (through ownership or leasehold custodianship), or is owned or leased by the user or a third party.
Malicious content may reside on, or be transferable from web content, electronic mail or analogous media.
It is a breach of this Policy to facilitate, whether deliberately or through negligence, the transfer of such material onto Brunel University London data network, or onto any machine connected thereto.
Equally, it is a breach of this Policy to facilitate the transmission of such material to other sites from or via Brunel University London data network. This includes the handling of any email suspected of the potential to contain such material, whether by explicit sending, automated redirection or the simple act of browsing the content. It also includes the proliferation by any means of spam and phishing messages.
This document, issued under the policies of the University, aims to clarify the security rules to be adopted by each user in the use of IT resources on the network access, access to the Internet, the use of University owned communication systems (e.g. email, enterprise social, network) and the use of IT Devices at its disposal to pursue their professional and academic activities.
These resources include computer equipment (including physical and virtual workstations, peripherals, physical and virtual servers and networks) and services (like email, Internet/Intranet, SharePoint, Office and Business Applications).

The set of security rules has to be applied in the following context:

- IT Devices and their contents are used to process information. IT devices managed by the University are used to process University classified information (see “Information Classification Policy” Information Classification Policy)
- University resources are dedicated to professional uses serving the interests of the University. However, the personal use of University resources like Internet access is tolerated to the extent that it remains reasonable, compliant to the local laws, not forbidden by specific security constraints (e.g. Prevent)
- University has established a security and safety organisation, procedures and safety systems which are described on IB and through security and safety awareness trainings

Brunel University London adhere to two guiding principles, Secure By Design Principles and Privacy By Design Principles to fashion and govern all IT infrastructure projects.

2.0 Acceptable Use Policy

2.1 Policy Framework

This Acceptable Use Policy is intended to provide a framework for such use of the University's IT resources. It should be interpreted such that it has the widest application and so as to include new and developing technologies and uses, which may not be explicitly referred to.

Cyber & Information Security and Information Services intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Brunel University London's established culture of openness, trust and integrity. Cyber & Information Security and Information Services are committed to protecting Brunel University London's employees, partners, students and the University from illegal or damaging actions by individuals, either knowingly or unknowingly. However, your awareness and cooperation is essential for maintaining the effective security of Brunel University London Information Systems.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and file sharing (SFTP) and Cloud services such as CHIME are the property of Brunel University London. These systems are to be used for University purposes in serving the interests of the University in the course of normal operations.

Information is an asset, and like any other business asset it has a value and must be protected. This value is not just financial but is based on the consequences of the information or Information Systems, being compromised and the negative impact that would have on individuals and The University. The University will continue to protect its interests against the inappropriate use of its Information Systems.

For the purpose of this policy, Information Systems is defined as Brunel University London systems, devices, services (e.g. Internet, email, "bring your own device" (when connected to the University systems) and telephony, applications and information in logical and physical form as well as any other University equipment. This also includes service providers' systems/equipment when provided to Brunel University London.

This Acceptable Use of Information Systems policy is part of the Information Security Policy Framework and should be read in conjunction with the Brunel Information Security Policy, Brunel University London Editorial Guidelines, Brunel University London Data Protection Handbook and any other relevant policies as mentioned in this document.

Any breach of industry good practice that is likely to damage the reputation of the JISC network will also be regarded prima facie as unacceptable use of the University Network.

Where the University Network is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the University Network.

2.2 Exceptions process

Where it is not possible to apply or enforce any part of this policy then a Brunel University London Dispensation Request must be completed and returned to Brunel University London Cyber & Information Security. Brunel University London Information Security will review the business justification and advise on the risks involved. Policy exceptions will only be issued when the Data Owner has signed off on the identified risks.

Exemptions for Unacceptable Use: There are a number of legitimate research, teaching and academic activities requirements that may be carried out using University information systems that could be considered unacceptable use. For example, research involving defamatory,

discriminatory or threatening material, the use of images which may depict violence, the study of hate crime, terrorism related material or research into computer intrusion techniques.

In such circumstances advice should be sought from the University's Legal Office (if potentially illegal material is involved) and/or notification made to the University Secretary via the procedure outlined in the University's Prevent Policy if the material relates to the promotion of extremism/terrorism prior to the introduction of said material onto the University network.

Any potential research involving obscene or indecent material must always be discussed in advance with the University's Legal Office. If a member of the University community believes they may have encountered breaches of any of the above, they should make this known to an appropriate University authority (such as the University Secretary, Director of HR, CIO or CISO).

2.3 Policy Compliance

Compliance Measurement

For security and network maintenance purposes, authorised individuals within Brunel University London may monitor equipment, systems and network traffic at any time.
Brunel University London reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

The Cyber & Information Security team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Non-Compliance

In the event of an apparent breach of the conditions of this Policy by a user, a group of users, or a user (or users) acting for such a group, the CISO, or designated agent, has the authority to:

- withdraw access to all or any subset of IS facilities from the user(s) and/or members of the group in question, or to commute such sanctions by issuing a warning of unacceptable use to the user(s) and/or members of the group in question
- restrict or terminate a User's right to use the University Network
- withdraw or remove any material uploaded by that User in contravention of this Policy
- where appropriate, disclose information to law enforcement agencies and take any legal action against a User for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith

Failure to respond to a warning, repeated breaches or serious transgression will result in immediate withdrawal of access to computing facilities.

In the event of the withdrawal of facilities, a report will be made by the CISO, or designated agent, to the user's college, department, similar unit of the University or relevant external body, except that in the case of an alumnus/a, the CISO (or a duly designated agent thereof) will have direct authority to suspend or delete any or all access privileges.

Recourse will be made to the University's usual disciplinary procedures, where it is deemed necessary by the CISO. Legal action may be taken by Brunel University London in any instance wherein it is deemed to be in the interests of the University to do so.

In addition, where the User is also a member of the University community, the University may take such action, disciplinary or otherwise as it deems appropriate and which is in accordance with its Charter, Statute, Ordinances and Regulations.

3.0 Network IS

The University adopts the principle of least privilege (PoLP) which is the practice of limiting access rights for users to the bare minimum permissions they need to perform their work. Under PoLP, users are granted permission to read, write or execute only the files or resources they need to do their jobs: In other words, the least amount of privilege necessary. Administrative privileges are only given to those authorised by IS, College IT or InfoSec with justifiable reasons.

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Legitimate University research and teaching may require exceptions for some of the listed unacceptable use controls (such as port scanning) on a short-term basis and will necessitate the cessation of the Acceptable Use Policy control. The re-establishment of the Acceptable Use control position will be expected upon completion of the research or teaching requirement. Ref.2.2)

Under no circumstances is an employee or student of Brunel University London authorised to engage in any activity that contravenes UK legislation or appropriate regulations while utilising Brunel University London-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use:

- You must not attempt to deactivate**,** bypass, tamper with or reconfigure any protection installed on any IT Device e.g. antivirus service, desktop firewall, services to install security patches or any other of the security measures that The University has in place
- You must not modify the configuration of University Information Systems nor install additional software unless you have been authorised to do so
- Only equipment that has been authorised by the University must be used to directly connect to the University Information Systems network
- You must not access data, a server or an account for any purpose other than conducting Brunel University London business
- You must not intentionally or recklessly introduce malicious programs or any form of spyware into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.)
- You must not make fraudulent offers of products, items, or services originating from any Brunel University London account
- You must not make statements about warranty, expressly or implied, unless it is a part of normal job duties
- You must not effect security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing,

pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes

- You must not engage in port scanning or security scanning
- You must not execute any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty
- You must not circumvent user authentication or security of any host, network or account
- You must not introduce honeypots, honeynets, or similar technology on Brunel University London network unless Cyber & information Security authorisation is given
- You must not interfere with or deny service to any user (for example, denial of service attack)
- You must not use any program/script/command, or send messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet
- You must not intentionally waste staff effort or other University resources
- You must not corrupt, alter or destroy another User's data without their consent
- You must not disrupt the work of other Users or the correct functioning of the University Network or deny access to the University Network and its services to other users
- You must not pursue any personal business or commercial activities whilst using University IT assets (Intranet sales & wants ads exempted)
- You must not introduce data-interception, password-detecting or similar software or devices to the University's Network
- You must not seek to gain unauthorised access to restricted areas of the University's Network nor seek access or try to access data where the user knows or ought to know that they should have no access
- You must not carry out any hacking activities
- You must not provide information about, or lists of, Brunel University London employees to parties outside Brunel University London unless authorisation and consent is given by the Data Protection Officer and HR
- You must not use wired and wireless connection in parallel to connect a device to the same network at the same time
- You must never connect any IT device on two networks at the same time unless authorisation has been given by Information Services for servers and network equipment
- You must not turn University information, staff information or students information into personal information
- You must not store University Confidential information on a mobile device unless encrypted
- You must not download or use software without a business need. Employees are explicitly prohibited from any use of the University IT for peer-to-peer file sharing,

downloading of copyrighted (unauthorised), illegal or offensive materials like games, music, films or entertainment programs

- You must not install software in violation of intellectual property laws or licenses
- You must not participate in any crypto-mining activity either using University IS equipment or using power provided by the University
- **No unauthorised use of** the University Identity for third party activities (i.e. working for a third party organisation)
- **No manipulation** of accounts, servers or network components to facilitate gaining unauthorised access to resources, or hijack or redirect network connections
- **No hacking of information or programs**. The voluntary access to information of any kind must be motivated by business need. Misuse, abuse or unauthorised access of accounts or passwords is prohibited. In particular access to the correspondence of others cannot be regarded as motivated by business need. The University prohibits the unauthorised access of its systems and networks. Violations may be subject to criminal and/or civil liabilities

The University Network may not be used directly or indirectly by a User for the download, creation, manipulation, transmission or storage of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material, this material includes but is not limited to:

- unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others
- material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of the University or a third party
- material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation
- material with the intent to defraud or which is likely to deceive a third party
- material which advocates or promotes any unlawful act
- material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party
- material that brings the University into disrepute

3.1 Anti-Virus

You must:

- Regularly check the proper operation and systematic updating of the antivirus ('right click' on the icon of the virus defense software or observe the antivirus icon in the status bar) and report to helpdesk any malfunction found or question
- Analyse a file that is downloaded or copied from an untrusted source to detect viruses ('right click' on the message and then 'Scan for viruses') before it is opened
- If a virus is identified on an IT Device and if it cannot be deleted by the antivirus software, the user should immediately disconnect the computer from the network

(physically disconnect the network cable and shutdown of wireless connectivity) and report the incident to the helpdesk

4.0 Email and Communication Activities

When using a Brunel University email account, whether on campus or remotely, staff should follow all the policies outlined in the Ref BUL-POL-EMAIL - Email Use Policy

5.0 Monitoring

General monitoring: Both specialist IT staff and automated computerised systems are used to monitor Brunel University London Information Systems including but not limited to Brunel University London telephones, email, mobile devices, computers, CCTV, communications systems, network traffic data and Internet systems. Systems have been implemented to automate monitoring where viable to ensure real-time protection and minimal human intervention. Digital information and data passing through these systems are subject to on-going and random monitoring for system security and integrity reasons in order to:

- maintain the effective operation of Brunel University London's communications systems
- check on standards of service and quality of staff performance
- ensure compliance with this policy

Specific monitoring: Your communications may be monitored when it appears that Brunel University London Information Systems are being misused or used inappropriately.

There may be other reasons why your communications are monitored, e.g. in your absence after a formal request is made for access to emails and/or data files in your mailbox or on your device to ensure business correspondence is dealt with. This will be in accordance with an authorised investigation. No monitoring of communications, such as during an absence, can be made by the authorised University administrator without prior approval from the Data Protection Officer, in accordance with current legislation including rights of employee representative bodies (HR / Unions). As exception from this principle authorised administrators may collect and use log data and results of security systems to detect, locate and eliminate faults and malfunctions or do forensic investigations.

Information privacy: Your personal privacy is respected and access controls are in place, but you must understand that The University may monitor your use of Brunel University London Information Systems for security purposes and also to check your compliance with this policy at any time and potentially without notifying you.

The University adopts the guidance outlined in the Information Commissioners' Employment Practices Code and the Lawful Business Practice Regulation Part 3 – Monitoring at Work. The latter describes how organisations can seek to ensure adoption of the principles of the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Brunel University London is ultimately responsible for all communications and devices on Brunel University London Information Systems. It is therefore important that you understand

that The University can investigate your Brunel University London communications and your use of its Information Systems for reasons which include:

- any serious incident where the investigation of The University, or its staff, is necessary in the public interest
- to comply with legal obligations and the prevention or detection of criminal activities
- to ensure that The University's policies and procedures are adhered to
- to prevent or detect unauthorised use of Brunel University London Information Systems
- when necessary, to conduct authorised investigations into an individual user

Investigation of past communications: Your past communications may be examined or analysed as part of on-going operational needs or investigations. The University may use any information it obtains via this process to investigate any claims of breach of this policy or any law and to instigate appropriate disciplinary or legal proceedings.

Notification of investigations: Wherever reasonable, and if appropriate, we will consult you about any suspected breach of this policy before any action is taken against you. However, it may not be practical to consult with you beforehand where illegal behaviour or gross misconduct is suspected.

Personal information during investigations: You should be aware that investigations may reveal personal information about you, for instance which websites you visit, the identity of people you email for personal reasons etc. This will be held in confidence unless it is needed to form part of an authorised investigation.

Monitoring personnel: Access to information obtained through monitoring is controlled and limited to trained and designated staff to ensure an acceptable level of confidentiality and privacy.

6.0 Harassment

Harassment is prohibited: The University will not tolerate any form of harassment and is committed to providing a workplace in which the dignity of individuals is respected. You must not knowingly attempt to send electronic communications or information on Brunel University London Information Systems which may be deemed by the recipient to violate dignity or be perceived as intimidating, hostile, degrading, humiliating or offensive, as set out in Brunel University London Bullying & Harassment Grievance Policy. Any harassment will be dealt with under Brunel University London's Disciplinary Policy and may result in disciplinary action being taken and could potentially be a criminal offence.

7.0 Defamation

Defamation is not allowed[1]: You must not send or circulate, internally or externally, any information that is defamatory**.** This includes any information that contains negative comments

[1] Defamation is the publication of a statement that adversely affects the reputation of a person or an organisation. The publication can be made using the Internet or any other electronic communication.
A person or organisation defamed can sue you or Brunel University London for damages. Although the law recognises that it is a defence if the information is 'true', the onus is on you or Brunel University London to show that there is also a defence of fair comment.

about an individual or organisation without first checking that the contents of the information are accurate.

8.0 Social Media / Blogging

You must use caution when using social media for communication. You must use social media sites in a professional and responsible manner and your contributions must comply with Brunel University London Social Media and Social Networking Guidelines.

When using any social media channel, staff should follow all the policies outlined in the BUL-POL-SOCIAL- Social Media Use Policy.

It is your responsibility to ensure the social media account is protected by enabling the privacy settings available.

9.0 Printing

When printing any University Confidential or Protect documents on printers make sure that no unauthorised person gain access to the documents.

Take all originals and copies with you after using a copying machine and destroy unneeded copies containing University confidential or protect information.

10.0 Passwords

Creation of strong passwords: You must create your unique passwords in accordance with the BUL-POL-9.4.3 - Password Policy.

Keep passwords secure: You must keep all your passwords safe. Don't write them down in any manner that would make it easy to decipher and don't tell anyone your login details or password – including your manager or IS. This also includes family and other household members when work is being done at home. Passwords on all information systems and websites i.e. social media must be kept secure. Any activity carried out on your password protected account will be deemed to be your activity unless there is evidence to the contrary

Revealing your account password to others or providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

Change passwords regularly according to the University password policy and ensure the secrecy of passwords and PINs. Also PINs have to be changed regularly where applicable.

We recognise there may be instances when you do need to share your password, however you must only do this with a valid business justification and only after notifying the University's CISO or CIO.

You must thereafter change your password at the earliest opportunity.

11.0 Classification - University Confidential and Protect information

Brunel University London proprietary information stored on electronic and computing devices whether owned or leased by Brunel University London, the employee or a third party, remains the property of Brunel University London.

You must ensure that all University information is classified correctly and marked appropriately in accordance with the BUL-POL-08-02 Information Classification policy.

You must take all the appropriate measures to ensure through legal or technical means that University Confidential information is protected in accordance with the BUL-POL-08-02 Information Classification policy and is compliant with Data Protection Legislation, e.g. by using encryption or ensuring its physical security.

Sending Restricted information: If you need to communicate any University Confidential information or information you consider sensitive then it must be encrypted. Further information

and guidance can be found in the BUL-PROC-08-02 Information Classification and the BUL-POL-10.1 - Cryptographic Policy.

12.0 Incidents and Damage

12.1 Information security incidents:[2] You must report all actual or suspected information security incidents immediately to the University's Cyber & Information Security team either directly or by email and/or phone.

Where the incident involves personal information then you must also immediately report the incident to the Data Protection Officer.

Reporting theft or loss: You must immediately report all lost or stolen Brunel University London

Information Systems, or other devices containing Brunel University London information, to your local IT Service Desk. Where the theft or loss of a physical item involves personal information then you must also immediately report the incident to contact the Data Protection Officer.

Incident Investigation: Brunel University London may investigate your communications and use of Brunel University London Information System for reasons outlined in this policy.

12.2 Damage and fault reports.

Brunel University London's computing facilities are provided for common usage to authorised users, each of whom needs to take reasonable steps to avoid damage or prolonged loss of service. Damage refers to any deliberate or accidental damage to any Brunel University London IS facility, including any modifications to hardware or software, which incur time or cost in restoring the system to its original state.

Users must not cause any form of damage to Brunel University London's IS facilities, nor to any accommodation or service related to them.

Installation (or modification of the setup) of software, or connection of hardware (including peripherals) to the data network of Brunel University London (whether directly or via another machine) must be with the explicit approval of the Chief Information Officer and in accordance with all local codes of practice.

Users should also take all reasonable steps to report any faulty equipment to the Information Services, and endeavour to leave computers in a clean, usable state.

13.0 Offensive material

You must not knowingly attempt to visit, send or store any website, electronic communications or information on Brunel University London Information Systems that is likely to cause harassment, alarm or distress. This includes sites and information which may contain nudity, pornographic, obscene, indecent, hateful or other offensive material. Authorisation to access such material for academic or research purposes must be applied for in advance through Line Management approval.

14.0 Remote access

When you use a public/shared device to access Brunel University London information remotely, you must reject any prompt to save your username or password in the browser for future use. You must also ensure that you log out of the remote access service completely when you are finished and close any open browser. Where possible you should log out of the device

[2] An event that is likely to compromise Brunel University London by putting the confidentiality, integrity or availability of its information at risk.

completely and either shut it down or restart the device. It is your responsibility to ensure that your remote access occurs in an appropriate environment.

You are responsible for University IS provided devices (laptops, mobile phones and other equipment) for professional and academic use. It is not permitted to share this equipment with any person(s), including members of the family.

15.0 Physical security

Access to premises: Access to Brunel University London premises is for authorised personnel only through the allocation of a Brunel University London Identity Card.

The University campus has two distinct areas, private and controlled accessible areas requiring Identity card permitted access (e.g. offices and Library) and open access areas (e.g. Lecture Centre). The Acceptable Use Policy applies to both areas but greater care, vigilence and awareness should be taken in the controlled areas.

Please be aware of those in your office area and report any suspicious behaviour to University Security.

Brunel University London Identity Card: Lost Brunel University London Identity Passes must be reported to the University Reception immediately so that the pass may be temporarily deactivated.

Access to Brunel University London premises may be recorded for security purposes through CCTV and access management systems. Any attempted unauthorised access to areas which are restricted for either security or health and safety reasons is a violation of this policy.

Keeping your desk clear: You must make sure all University Confidential and Protect information is locked away when you leave the office in accordance with the University's clear desk policy.

Protecting your equipment: You are responsible for ensuring the security and safe keeping of Brunel University London Information Systems and other devices containing Brunel University London information particularly at non-Brunel University London locations such as your vehicle, at home, when on the train, having a coffee etc.

Safe storage: If you need to leave any portable Brunel University London Information System (such as phones, mobiles, laptops and tablets), or any other device containing Brunel University London information, in the office overnight or when you have finished working for the day, then you must lock it into storage. If you are at a non-Brunel University London location then you must take similar measures.

Protecting your screen: If you need to leave your PC or other mobile device containing University information unattended then you must immediately activate a password protected screen lock or PIN security.

Shutting-down your computer: You must always shut-down your computer, and wait until it has fully shut-down, when you have to leave it unattended for long periods of time or when not using it outside of your normal working hours.

Using removable storage[3]: If you are copying University Confidential information to removable storage media (e.g. USB drives, CD/ DVDs etc.) then you must encrypt it in compliance with the BUL-POL-10.1 - Cryptographic Policy and BUL-POL-08-02 Information Classification and keep it secure at all times.

Removable storage from third parties: You must advise any third party wishing to send you any University Confidential information on removable media to use encryption as outlined in our BUL-POL-10.1 - Cryptographic Policy. If you have received the removable media unencrypted

[3] USB disk, CD/DVD, Memory Card, Smartphone disk

then you must copy the information to your Brunel University London Information System and immediately encrypt the removable media.

Shoulder surfing: In open or public places, such as the library, teaching areas, trains or coffee shops, you must be aware of others who may be able to view your password entry, screen or papers. You must take appropriate precautions particularly with using University Confidential information in such circumstances.

For University provided laptops, an effective use of an additional locking security cable (e.g. Kensington Lock) is required at any time the laptop is not under visual control. If no locking security cable is available the laptop has to be locked in an office cupboard.

16.0 Data Protection

The use of the IT resources by users imply the collection and processing of personal data as defined under the EU Directive, **General Data Protection Regulation** which applies in the UK from May 2018 which supersedes the **Data Protection Act 1998** on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Where personal data are collected and processed, users are duly informed of the purposes and means of processing. In such situations, University commits that the data will be compliant with Article 5 of the GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and

organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Users are granted with a right to access, rectify or erase the data which are collected and stored. They can exercise this right by contacting the Data Protection Officer.

17.0 Logs information

IT and communication systems rely on logs which are mostly generated automatically by IT and telecommunications equipment. This logging information is stored on workstations, Servers, Applications and on network appliances.

Personal Identifiable Information related log information will be erased if the purposes for which they are collected are no longer applicable.

18.0 Legislative and Copyright

The following activities are strictly prohibited, with no exceptions:

Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Brunel University London.

Copyright: You must not download, store, copy or transmit the works of others without their permission as this may infringe copyright. If you use someone else's copyright protected material without their consent, you may be guilty of an offence under the Copyright, Designs and Patents Act 1988.

Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Brunel University London or the end user does not have an active license is strictly prohibited.

It is your responsibility to ensure that you remain compliant with ***all*** UK legislation and regulatory frameworks whilst engaged in working on University IT. Ref. BUL-POL-LEGIS - Legislative and Regulatory Framework Policy.

19.0 Reputational damage

Consequent on any breach of information security, or following any instance of poor online behaviour by a Brunel University London account-holder, including an account-holder for a facility managed on behalf of Brunel University London by any third party or attributable to an entity on the internet managed by Brunel University London (for example, an IP address assigned to Brunel University London), there is a risk of reputational damage to Brunel University London. This may include automated or manual inhibition of service to and from Brunel University London, the invocation or creation of penalty clauses within contracts, or general deprecation of Brunel University London within the internet citizenry. Such reputational damage hurts the University seriously, quickly, and potentially for a long period of time. The endangerment of Brunel University London's online reputation is a serious breach of this Policy, and disciplinary proceedings may be instituted against any user who, whether deliberately or negligently, exposes Brunel University London to such risk. Legal redress will be sought where and when appropriate.

20.0 Staff Personal use

You are permitted to use the University's communications services, including but not limited to telephones, mobile phones and Skype, for a reasonable amount of personal use, however this

must be kept to a minimum since the communication services must be kept available for business use. Any abuse of the communications service, such as excessive, long, premium or long-distance usage may result in disciplinary action. If you have an exceptional circumstance then you must seek authorisation from your line manager.

In addition to communication services, you are allowed reasonable and limited personal use of University provided IT equipment and services provided.

The use of University emails is limited to University related business, the use of University emails for personal and private use is not allowed, but incidental and reasonable use of University emails for private or personal use will be tolerated.

The University may decide to limit your ability to use University Information Systems for personal use where there is possible, or actual, interference with Brunel University London business. This would be decided by your line manager with input from Brunel University London HR.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments and Colleges are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

The use of University provided IT equipment for any commercial or business activities or used to take part in online gambling which are not related to your work at the University is strictly prohibited.

Any personal or not-for-profit exploitation of university computing resources — if permitted at all — will be strictly controlled. Personal (i.e. non-University provided) accounts must be used for correspondence and personal business which does not meet the conditions of bona fide Brunel University London business as outlined above.

Such use which impinges on IS facilities and services of Brunel University London — even as minimally as using a networked printer — may cause infringements which could render the University liable to prosecution. Personal or group solicitation on behalf of third parties, whether commercial, non-profit, political, religious, charitable or individual, is similarly beyond the scope of acceptable use of a Brunel University London account, including an account provided by Brunel University London but managed on behalf of the University by any third party.

Any user contemplating such personal, not-for-profit or commercial use must, therefore, contact their Department Head or College Director in advance to seek consent, and must demonstrate that there is no other avenue, such as the use of personal non-University accounts and of (free or paid-for) cloud store.

It is strictly prohibited to use University IS services or equipment for the purpose of solicitation on behalf of a third party (including commercial, charitable, religious or political entities), or for one’s own preferment in any such endeavour.

21.0 Software & Mobile Apps

Unauthorised software: The integrity and security of the University and its Information Systems could be impacted by downloading unauthorised, illegal or malicious software.

You must not knowingly download, install or run any software on a Brunel University Information Systems provided server or Endpoint without first obtaining appropriate authorisation (by contacting IS), unless the software is listed as approved on the Software Catalogue. College IT systems provided for legitimate research and teaching will be responsible for the appropriate College exemption authorisation.

If you need to install software (for example to complete specific directed tasks) you must make every effort to inform your Manager and Information Security in advance and seek guidance.

When this is not possible (for example outside normal working hours) they must inform their managers and Information Security by e-mail and ensure that the software is removed immediately after the specific task is completed.

Mobile applications: You must only download or install mobile applications onto Brunel University London Information Systems from approved and reputable sources such as an official application store or market. The integrity and security of the University and its Information Systems could be impacted by downloading unauthorised, illegal or malicious software. Further requirements on the use of mobile devices can be found in the Remote Working Policy.

You must read the information about an application in the application store before you download it and make sure that you are happy with the information it will be accessing.

No application not of Brunel University London's management may be used if it has a feature which seeks to capture and store Brunel University London information. If you are in any doubt about whether to download an application, please contact the Cyber & Information Security team.

22.0 Behaviour

Users of computing facilities at Brunel University London should always act with consideration and respect for the staff, students, other users and the equipment provided — hardware, software, fittings and furniture, and all other assets.

You must act honestly and with integrity at all times to protect the University's reputation, in accordance with Brunel University London values.

Your role: You must understand your role and responsibilities with regard to Brunel University London Information Systems and to your role as an information asset owner (BUL-POL-6.1.2 - ISMS Asset owners Roles and Responsibilities). If this is unclear then you must consult your line manager.

When accessing Brunel University London Information Systems you must only carry out the activities you are authorised to do. You must not access or try to access any Brunel University London information Systems where you are not authorised to do so, for example logging into accounts which are not yours. Doing so may be a crime under the Computer Misuse Act 1990.

You are responsible for any activity carried out under your username. You must not let anyone else use your Brunel University London Information System when logged in with your own username and password unless all of the following apply:

- it is for IT support or delivering presentations/training where multiple people need to use one device
- it is for a limited period of time
- it takes place under your direct and continuous supervision

You have a responsibility to promptly report the theft, loss or unauthorised disclosure of Brunel University London proprietary information.
You may access, use or share Brunel University London proprietary information only to the extent it is authorised and necessary to fulfil your assigned job duties.

Users should be considerate of others' legitimate use of computing facilities and the rights of all users to work undisturbed must be respected.

University Windows PCs are secured with a password-protected screensaver with the automatic activation feature set to 20 minutes or less. You must lock the screen or log off when the device is left unattended.

Ensure machines are left available to others when leaving a computer for a break (however short), by logging out. This will protect your work as much as helping other users. It is an

offence against this Acceptable Use Policy for any user to lock access to any PC or workstation in any public-access workarea, kiosk location, or similar facility, or to leave such a device unattended while logged in. Staff of the Information Services, and their duly authorised agents, have the authority to close any unattended session on any PC or workstation in a public-access workarea, kiosk location, or similar facility.

Often, a computer workarea is booked for teaching purposes and sometimes this leaves machines in these areas unused. You may be allowed access to one of these machines but this will be only with the consent of the staff member(s) in charge of the booked session. Staff running such booked sessions must remain aware of the demand for PC/workstations and, unless there are over-riding considerations (such as the need for security of a session being undertaken under examination conditions), should allow access to any unused machines. If you are allowed access to a spare machine during a booked session, you should display appropriate behaviour (i.e., by respecting the primacy of the booked session, by making no noise and by remaining as unobtrusive as possible). If you prove to be a distraction to participants of the booked session, you will be asked to leave by the staff member(s) in charge of the booked session, and you should do so without question or argument and with a minimum of disturbance.

Observe opening and closing times, leaving promptly when requested for booked sessions or closure.