BRUNEL
SEN MAT

STAFF ACCEPTABLE USE POLICY

Introduction

The purpose of this document is to ensure that all users (including but not limited to Employee, Students, Visitors, and Contractors) are aware of Establishment policies relating to their use.

The establishment encourages the use of computing (and other technologies, referred to as 'ICT Facilities') for the benefit of its users. The computing resources are provided to facilitate a person's work as a user of the establishment, specifically for educational, training, administrative or research purposes. The regulations that constitute this policy seek to provide for the mutual protection of the establishment and the rights of its users.
Effective and proper use of information technology is fundamental to the successful and efficient running of the Establishment. However, misuse of information technology – in particular misuse of e-mail, internet and social media – exposes the Establishment to liability and is a drain on time and money.
Whilst the traditions of academic freedom will be fully respected, it is the responsibility of all users of the Establishment ICT facilities to be aware of, and follow Establishment ICT polices and guidelines and to seek advice in case of doubt.

2. ICT Facilities

2.1 Access to ICT facilities are managed by IT Services. Use of ICT facilities is at the discretion of IT Services and the establishment Senior Management (referred to as 'SMT')

2.2 **Definitions**

2.2.1 The phrase 'ICT Facilities' as used in Establishment policies are interpreted as including any computer hardware, printers, telephones, or software owned or operated by the Establishment, including any allocation of memory/disk space on any of the Establishment systems.

2.3 **Ownership**

2.3.1 ICT facilities owned by the Establishment and software and/or data developed or created (for whatever reason) on that equipment remains in all respects property of the Establishment. The Patents Act 1977 and Copyright, Design and Patents Act 1998 provide for the Intellectual Property Rights (IPR) in that work created by an employee in the course of his/her employment is vested automatically to the employer.

2.4 **End User Devices (Desktop PCs / Laptops / Mobile Devices)**

2.4.1 End User Devices are a critical asset to the Establishment and must be managed carefully to maintain security, data integrity and efficiency.

2.4.2 IT Services has measures in place to prevent installation of software, but users must consult IT Services before attempting to purchase and install non-standard software on establishment devices.

2.4.3 All users have access to appropriate areas on the Establishment's file servers for the secure storage of valuable files.

2.4.4 Laptop & Mobile devices are at a high risk from loss or theft and require additional security protection. All reasonable precautions must be taken to ensure that the hardware is stored securely.

2.4.5 To protect the integrity of the Establishment systems and data procedures, passwords or authentication devices for gaining remote access to the Establishment systems must not be stored with the computer. This includes the saving of passwords into remote access software.

2.4.6 Confidential data should not be taken offsite via removable media / etc. Remote Access provides a secure VPN (Virtual Private Network) system which is highly encrypted and secured. If there is a requirement to take any confidential data offsite then please discuss with Central Services and IT, to ensure the Establishment's Data Protection obligations are met.

2.4.7 In event of loss or theft of a device you should report the matter promptly to Central Services and IT to enable access to establishment systems by a device or user to be revoked and/or the activation of a remote locate and wipe facility operated by the establishment.

2.4.8 All portable device must be handed back in good condition in order for redistribution along with associated power supplies and accessories. If the device is not in a reasonable condition, the user may be liable for its repair or replacement.

2.4.9 All IDs, usernames, passwords and passcodes for devices must be supplied before leaving the establishment so the relevant devices can be wiped and repurposed. Failure to do this may result in the user being liable for the cost of the device.

2.5 **Loan Equipment**

2.5.1 The policy regarding loan equipment is similar to that for laptops and mobile devices. Most loan equipment is highly portable and attractive to thieves. Users who borrow loan equipment should sign for it (or obtain a parental signature) and bear the responsibility of its care. Loan equipment should be concealed and stored securely when not in use.

2.5.2 If loan equipment is stolen or lost you should report the matter promptly to Central Services and IT to enable access to establishment systems by a device or user to be revoked and/or the activation of a remote locate and wipe facility operated by the establishment.

2.5.3 If damage occurs to loan equipment, please inform the IT services – you should not attempt to fix or have the device repaired yourself.

2.6 **ICT Disposal**

2.6.1 All ICT equipment must be disposed of by IT Services using a WEEE certified disposal company. All disposal documentation shall be kept within IT Services.

2.7 **Software**

2.7.1 IT Services has measures in place to prevent installation of software, but users must consult IT Services before attempting to purchase or install non-standard software on establishment devices.

2.7.2 Only software properly purchased and/or approved by IT Services may be used on establishment hardware. Non-standard or unauthorised software can cause problems with the stability of establishment ICT facilities.

2.7.3 Mobile Apps loaded onto Establishment owned “tablet” devices are the responsibility of the user in terms of configuration and licensing. IT Services will support Apps on a “best endeavor” basis.

2.8 **Network Access**

2.8.1 In order to use the ICT facilities of the Establishment a person must first be provided with their own user name by IT Services. Registration to use the computer facilities implies, and is conditional upon, acceptance of this Acceptable Use Policy. Staff users will be created upon receipt of a New User request from the HR Department. Student accounts will be created at the start of term via information contained within the establishment MIS System.

2.8.2 All individually allocated usernames and passwords are for the exclusive use of the individual to whom they are allocated. Passwords protect the Establishment’s systems from access by unauthorised people; they protect your work and the Establishment’s information. The user is personally responsible and accountable for all activities carried out under their username.

2.8.3 The password associated with a particular personal username must not be divulged to another person, except to trusted members of IT services. (The member of IT services will then show you how to re-set your password so that they no longer know it.) Attempts to access, or use, any username, which is not authorised to the user are prohibited.

2.8.4 Passwords have to be complex and must therefore:
a. Be at least six characters in length;

b. Contain characters from three of the following four categories:
i. English uppercase characters (A through Z)
ii. English lowercase characters (a through z)
iii. Base 10 digits (0 through 9)
iv. Non-alphabetic characters (for example, !, $, #, %)
c. Not contain the user's account name or parts of the user's full name that exceed two consecutive characters e.g. not contain “Ash” if you happen to be a “Ashton”.
d. Examples: B@bsfc1, C@claughtonCH43, Ilovec00l3ge, etc

2.8.5 IT Services does not allow the connection of non-establishment computer equipment to the network without prior written request and technical approval. This includes connection via dialup or Virtual Private Networking (VPN). This however excludes connecting devices via the Establishment’s BYOD (Bring Your Own Device) network.

2.8.6 It is establishment policy to store data on a network drive or the Onedrive where it is regularly backed up. IT service will not be responsible for data stored outside these areas. eg: C:\ drive

Valued documents and files should not be stored on Desktop PCs or laptops. Files stored on Desktop PCs are at risk of loss through hardware/software failure or automated administrative activity.

2.8.7 The Establishment maintains a notification with the Information Commissioner’s Office in compliance with the Data Protection Act 1998. It is the responsibility of all Establishment staff to ensure that personal data held and processed is within the terms of the Establishment’s data protection policy.

2.8.8 Under no circumstances should you disclose personal or other confidential information held on computer to unauthorised persons. The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computers’ Misuse Act 1990.

2.8.9 Old Student Accounts will be disabled during the first term. The data files relating to this account will be retained for 1 year as part of the Establishment backup policy.

2.8.10 Old Staff Accounts will be disabled on the last day of service. It is the responsibility of the staff member to gather any relevant data, files and e- mails they require during their notice period. This data can be copied by IT Services upon request. The files relating to this account will be retained for 6 months

2.9 **Wireless Access**

2.9.1 The Establishment supplies two different levels of wireless access; Establishment Devices and guest devices

2.9.2 Establishment Devices is configured on establishment owned devices by IT Services. This is setup and authentication credentials are known only to IT Services. Devices connected via "Establishment Mobile" wireless are treated exactly as a wired desktop PC and as such need to be protected.

2.9.3 Guest access is open to any wireless client. Clients connecting to guest access will need to obtain the key prior to connecting.

2.9.4 Guest access has been limited to only allow access to Internet and other web-based technologies such as E-Mail. Access to file shares (such as network drives) are not permitted and controls are in place to prevent it.

3. Data Security

3.1.1 You must only access information held on the Establishment's computer systems if you have been properly authorised to do so and you need the information to carry out your work.

3.1.2 It is establishment policy to store data on a network drive where it is regularly backed up.

Valued documents and files should not be stored on Desktop PCs or laptops. Files stored on Desktop PCs are at risk of loss through hardware/software failure or automated administrative activity.

3.2 **Personal Data and the Data Protection Act**

3.2.1 The Establishment maintains a notification with the Information Commissioner's Office in compliance with the Data Protection Act 1998. It is the responsibility of all Establishment staff to ensure that personal data held and processed is within the terms of the Establishment's data protection policy.

3.2.2 Under no circumstances should you disclose personal or other confidential information held on computer to unauthorised persons. The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computers' Misuse Act 1990.

3.3 **Freedom of Information Act**

3.3.1 The Establishment is subject to the provisions of the Freedom of Information Act (2000) which provides for the general right of access to information held by public authorities.

Employees should be aware that the Act effectively extends rights available under the Data Protection Act to include all types of information held, whether personal or non-personal. Requests will be dealt with according to the Establishment Freedom of Information Policy.
3.3.2 Staff should note that all data and correspondence, including e-mail messages, held by the Establishment may be provided to a data subject, internal or external, in the event of a subject access request.

3.4 **Anti-Virus / Anti-Spam Protection**

3.4.1 Anti-virus software is loaded on all computers as standard and is updated regularly via the network. There are security protocols in place to prevent users from attempting to remove or de-active the Anti-Virus software, so please do not attempt to do so.

3.4.2 Non-Establishment software or data files intended to be run on establishment equipment by external people such as engineers or trainers must be checked for viruses before use. If you suspect that a virus has infected a computer then stop using the computer and contact IT Services immediately. As soon as a Virus is detected on an external device (such as a USB), IT Services are immediately emailed (and an automatic clean-up is attempted).

3.4.3 Files received by or sent by e-mail are checked for viruses automatically.

3.4.4 USB drives are permitted but will be read only on the network and must be encrypted.

3.4.5 Computers and email accounts are the property of the Establishment and are designed to assist in the performance of your work. You should, therefore, have no expectation of privacy in any email sent or received, whether it is of a business or personal nature.

4. E-Mail

4.1 **Use and Responsibility**

4.1.1 Staff - The Establishment's email system is provided for the Establishment's business purposes and academic support. Limited personal use of the email system is permitted, but not to a level that would influence the primary business purpose. The Establishment will be held liable for any contractual arrangements entered into by email by members of staff if it is reasonable for the recipient to assume that such people are acting with authority (employer's vicarious liability). Such commitments should be avoided at all costs unless specifically authorised.

4.1.2 You should not use your establishment email if purchasing personal goods.

4.1.3 The email system costs the establishment time and money and it must be used judiciously in the same manner as other establishment resources such as telephones and photocopying.

4.1.4 Establishment-wide email messages must be business related and of significant importance to all employees. Non-Establishment email accounts should not be used for conducting Establishment business unless in an emergency situation.

4.2 **Content**

4.2.1 Email messages must be treated like any other formal written communication. Improper statements in email can give rise to personal liability and liability for the Establishment and can constitute a serious disciplinary matter.

4.2.2 Email messages to or from you cannot be considered to be private or confidential.

4.2.3 Email can be copied and forwarded to numerous recipients quickly and easily and you should assume that they could be read by anyone.

4.2.4 Consider carefully before sending confidential or sensitive information via email. Email messages, however confidential or damaging, may have to be disclosed in court proceedings. Please consult IT Services for advice.

4.2.5 Do not create or send email messages that may be intimidating, hostile or offensive on the basis of sex, race, color, religion, national origin, sexual orientation or disability. It is never permissible to subject another person to public humiliation or ridicule; this is equally true via email.

4.2.6 Copyright law applies to email. Do not use e-mail to transmit or circulate copyrighted materials.

4.3 **Privacy**

4.3.1 Email messages to or from you cannot be considered to be private or confidential. Establishment emails will be regarded as the joint property of the Establishment and the individual staff member or student.

4.3.2 Although it is not policy to routinely examine the content of individual emails. The establishment reserves the right to monitor messages, at any time, for specific instances in which there is good cause for such monitoring or legal obligation to do so. Good cause shall include the need to fulfil legislative obligations, detect employee/student wrongdoing, protect the rights or property of the establishment, to protect the Establishment ICT system security, to obtain essential business information after reasonable efforts have been made to contact the mailbox user or to comply with legal process.

4.3.3 Emails are routinely scanned for the use of offensive language.

4.3.4 Messages sent or received may be copied and disclosed by the Establishment for lawful purposes without prior notice. Requests for access/monitoring unless required by law will only be authorized by a member of SMT.

4.3.5 It is not permissible to access or to send email from another users account either directly or indirectly, unless you obtain that person's prior written approval and a note is made with IT Services.

5. Internet

5.1 **Internet**

5.1.1 All Internet usage from the Establishment network is monitored and logged. Reporting on aggregate usage is performed on a regular basis. When specific circumstances of abuse warrant it, individual web sessions will be investigated and linked to the relevant user account. Such an investigation may result in action via the Establishment's Disciplinary Procedure and possibly criminal investigation.

5.1.2 Copyright and licensing conditions must be observed when downloading from the internet.

5.1.3 Once information is published on the worldwide web anyone from anywhere in the world can access it. It is therefore critical that material of a proprietary or sensitive nature should not be published on unsecured public web sites.

5.1.4 The Establishment reserves the right to remove access to any site(s) which it feels may inhibit the primary business purpose of Establishment.

Personal comments about members of staff and students are not acceptable. If in any doubt about other specific usage of such site(s) then discuss the matter with your Head of Faculty/Line Manager or, in the case of students, your tutor.
5.1.5 Instant messaging is free, fast, real-time and powerful. However instant messaging also carries inherent risks: lack of encryption (allowing the possibility of eavesdropping) logging of chat conversations without a user's knowledge and virus risks. Due to these risks, the Establishment does not currently allow the use of instant messaging for the communication of sensitive or proprietary Establishment information.

6. Private use, legislation and updates to this policy

6.1 **Private Use**

6.1.1 ICT facilities are provided for the Establishment's business and educational purposes and responsible personal use is therefore allowed provided there is no conflict with the interest or requirements of the Establishment.
6.1.2 The Establishment does not accept liability for any personal loss or damage incurred through using the ICT facilities for private use.

6.2 **Legislation**

6.2.1 The following are a list of Acts that apply to the use of the Establishment's ICT facilities:

Regulation of Investigatory Powers Act 2000
Computers' Misuse Act 1990
Protection from Harassment Act 1997
Sex Discrimination Act 1975
Race Relations Act 1976
Disability Discrimination Act 1995
Obscene Publications Act 1959
Telecommunications Act 1984
Protection of Children Act 1978
Criminal Justice Act 1988
Data Protection Act 1998
The Patents Act 1977
Copyright, Designs and Patents Act 1988
Defamation Act 1996
Freedom of Information Act 2000
Human Rights Act 1998

6.3 **Updates to this Policy**

6.3.1 In the light of changes in the business, technology, legislation or relevant standards it may be necessary to update this policy from time to time. Notification to all staff will be made when updates are available.

This policy has been adopted by Churchward School:

Signed …….. Headteacher

Signed …….. Chair of Governors

Date ……..