

## EMPLOYEE ACCEPTABLE USE POLICY

<b>AREA:</b>	<b>ICT</b>
<b>AUDIENCE:</b>	<b>ALL STAKEHOLDERS</b>
<b>REVIEW FREQUENCY:</b>	<b>1 YEAR</b>
<b>DATE ISSUED:</b>	<b>12.02.2019</b>
<b>LAST REVIEW DATE:</b>	<b>SEPTEMBER 2022</b>
<b>NEXT REVIEW DATE:</b>	<b>SEPTEMBER 2023</b>
<b>OWNED &amp; REVIEWED BY:</b>	<b>HEAD OF ICT</b>
<b>APPROVED BY:</b>	<b>CHAIR OF BRUNEL BOARD OF TRUSTEES</b>
<b>APPROVAL DATE:</b>	<b>22.09.2022</b>

*Brunel Academies Trust (Brunel) is a company limited by guarantee with registration number 10074054 and registered offices at Unit B4C Orbital Retail Park, Thamesdown Drive, Swindon, SN25 4AN; Brunel is the parent company and Sole Corporate Member of the subsidiary company, Brunel Education (BE), a company limited by guarantee with registration number 11991915 and registered offices also at Unit B4C Orbital Retail Park, Thamesdown Drive, Swindon, SN25 4AN.*

*The Brunel Education (BE) Board have approved and adopted the majority of Brunel Tier 1 policies and procedures. Tier 1 policies are centrally held policies relating to Governance, People Services, Finance, ICT and Operations and are the direct responsibility of Brunel. Tier 1 policies are created by the Brunel Central Services Team but adopted and reviewed by the Brunel Board.*

*Where this Brunel Tier 1 policy refers to Brunel this also therefore consistently applies to BE.*

### 1. Introduction

The purpose of this document is to ensure that all Employees, Child and Young Persons (CYP), Visitors, and Contractors are aware of Brunel Academies Trust (Brunel) policies relating to their use.

The Brunel 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 Brunel, specifically for educational, training, administrative or research purposes. The regulations that constitute this policy seek to provide for the mutual protection of the Brunel and the rights of its users.

Effective and proper use of information technology is fundamental to the successful and efficient running of the Brunel. However, misuse of information technology – in particular misuse of e-mail, internet and social media – exposes the Brunel 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 Brunel ICT facilities to be aware of and follow Brunel ICT policies and guidelines and to seek advice in case of doubt.

## **2. ICT Facilities**

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

### **Definitions**

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

### **Ownership**

ICT facilities owned by the Brunel and software and/or data developed or created (for whatever reason) on that equipment remains in all respects property of the Brunel. 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 their employment is vested automatically to the employer.

### **End User Devices (Desktop PCs / Laptops / Mobile Devices etc.)**

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

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 Brunel devices.

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

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.

To protect the integrity of the Brunel systems and data procedures, passwords or authentication devices for gaining remote access to the Brunel systems must not be stored with the computer.

Confidential data should not be taken offsite via removable media and measures are in place to stop data being written to such devices. If there is a requirement to take any confidential data offsite then please discuss with Central Services and IT, to ensure the Brunel's GDPR obligations are met.

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

All portable devices 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.

All IDs, usernames, passwords and passcodes for devices must be supplied before leaving the Brunel 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.

### **ICT Disposal**

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.

### **Software**

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 Brunel devices.

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

### **Network Access**

In order to use the ICT facilities of the Brunel a person must first be provided with their own username by IT Services. Registration to use the computer facilities implies, and is conditional upon, acceptance of this Acceptable Use Policy. Employee users will be created upon receipt of a New User request from the PS Department.

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

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.

Passwords are to be changed every 90 days, and must also:

- Be at least six characters in length
- Contain characters from three of the following four categories:
- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (for example, !, \$, #, %)
- Not contain the user's account name or parts of the user's full name

It is Brunel policy to store user data on a shared network drive, SharePoint or the OneDrive where it is regularly backed up. IT service will not be responsible for data stored outside these areas. Under no circumstances should you disclose personal or other confidential information held on computer to unauthorised persons.

Old accounts will be disabled on the last day of service. It is the responsibility of the employee 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.

### **Wireless Access**

The Brunel supplies two different levels of wireless access; Brunel Devices and guest devices.

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

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**

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

It is Brunel policy to store data only shared drives, SharePoint and user OneDrive area where it is regularly backed up.

### **Personal Data and GDPR**

It is the responsibility of all Brunel employees to ensure that personal data held and processed is within the terms of the Brunel's GDPR data protection policy.

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.

### **Freedom of Information Act**

The Brunel 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 Brunel Freedom of Information Policy.

Employees should note that all data and correspondence, including e-mail messages, held by the Brunel may be provided to a data subject, internal or external, in the event of a subject access request.

### **Anti-Virus and Protection**

Anti-virus and anti-malware 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 deactivate the Anti-Virus software, so please do not attempt to do so.

Non-Brunel software or data files intended to be run on Brunel equipment by external people such as engineers or trainers must be checked for viruses and malware 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).

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

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

Computers and email accounts are the property of the Brunel 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.

All computers are encrypted using a 'bitlocker' to protect data on the local hard disks of the computer in case of theft.

## **4. E-Mail**

### **Use and Responsibility**

Employees - The Brunel's email system is provided for the Brunel'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 Brunel will be held liable for any contractual arrangements entered into by email by employees 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.

You should not use your Brunel email if purchasing personal goods.

The email system costs the Brunel time and money and it must be used judiciously in the same manner as other Brunel resources such as telephones and photocopying. Brunel-wide email messages must be business related and of significant importance to all employees. Non-Brunel email accounts should not be used for conducting Brunel business unless in an emergency situation.

## **Content**

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 Brunel and can constitute a serious disciplinary matter.

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

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

Consider carefully before sending confidential or sensitive information via email. Email messages, however confidential or damaging, may have to be disclosed in court proceedings. Any emails containing sensitive information must be encrypted when sending to users outside the trust with attachments having password protection where possible.

Do not create or send email messages that may be intimidating, hostile or offensive on the basis of sex, race, colour, 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.

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

Emails should be checked for legitimacy to ensure that the emails are not from a bogus sender which could contain malware or phishing content. If you are not 100% sure the email is legitimate, advice should be sought.

## **Privacy**

Email messages to or from you cannot be considered to be private or confidential. Brunel emails will be regarded as the joint property of the Brunel and the individual employee member or CYP.

Although it is not policy to routinely examine the content of individual Brunel emails. The Brunel 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/CYP wrongdoing, and protect the rights or property of the Brunel, to protect the Brunel 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.

Emails may be scanned for the use of offensive content.

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

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

## **5. Internet and E-Safety**

All Internet usage from the Brunel network is filtered, monitored and logged using a Sophos XG Firewall which is managed and maintained by Wave 9. Designated users are then responsible for checking web usage reports and acting appropriately.

User activity is monitored across all computers for safeguarding purposes. This is done in the form of software which will continuously scan all programs on Brunel/BE devices and monitors for specific safeguarding keywords, with a screenshot captured of the device once the keyword has been typed or found on the screen. The screen shot is then sent to the safeguarding monitoring software for review by ICT, with any entries of concern passed to the safeguarding leads of the relevant provision.

Users must always act responsible when using Brunel devices, software, Internet and email and when specific circumstances of abuse warrant it, user accounts will be investigated. Such an investigation may result in action via the Brunel's Disciplinary Procedure, that may result in criminal investigation. No attempt should be made to bypass Brunel computer systems, Safeguarding measures, firewall and filtering.

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

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 websites.

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

Personal comments about employees and CYPs 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 CYPs, your tutor.

## **6. Private use, legislation and updates to this policy**

### **Private Use**

ICT facilities and devices are provided for Brunel's business and educational purposes only.

For safeguarding reasons, personal mobile phones are not permitted in the classroom or around the provision and must be kept in a secure location. Personal mobile phones can be used in emergencies or outside of the building away from children at break and lunch times.

Brunel does not accept liability for any personal loss or damage incurred through using the ICT facilities for private use nor does it accept liability for personally owned devices.


### **Updates to this Policy**

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 employees will be made when updates are available.

**This policy is adopted by the Brunel and will be reviewed annually or earlier if change to legislation.**

Signed: 

CEO

Signed: 

Chairman of Brunel Board

Date: 22 September 2022