

ACCEPTABLE ICT USAGE FOR STAFF POLICY

Date to be implemented from:	August 2026
Date to be reviewed by:	July 2027
Version No:	v11
Lead responsibility:	Directors

Distribution to:

All Staff	✓
SLT only	•
Teaching Staff/Tutors	•
Administration Staff	•
Other (please specify)	✓ Visitors, contractors

Key Contacts:

Directors	01438 727667

This Policy supersedes any previous Policy of this name or instructions that pre-date this edition.

ACCEPTABLE ICT USAGE FOR STAFF POLICY

1 Policy Statement

Members of Barrett-Bell Ltd and all other users (Staff, visitors, contractors etc) of the company's facilities are bound by the provisions of its Policies, including this Acceptable ICT Usage Policy. Barrett-Bell Ltd seeks to promote and facilitate the positive and extensive use of Information Communication Technology (ICT) in the interests of supporting the delivery of learning, teaching, innovation, research and administration tasks to the highest possible standards. Barrett-Bell Ltd will ensure that no member of Staff is at a disadvantage regarding IT access. All IT equipment will be recorded on the Asset Management Register and Staff must sign for any hardware allocated or borrowed.

2 Principles

- 2.1 This Acceptable Internet Usage Policy covers the security and use of all Barrett-Bell Ltd's information and IT equipment. It also includes the use of email, Internet browsing and research, downloading, gaming, subscription to blogs and sub-stacks, voice and mobile IT equipment.
- 2.2 This Policy applies to all Barrett-Bell Ltd's employees, contractors and contractor's agents and visitors.
- 2.3 This Policy applies to all electronic information, in whatever form (including paper copies of documents/emails), relating to Barrett-Bell Ltd business activities and to all information handled by Barrett-Bell Ltd relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by Barrett-Bell Ltd or on its behalf.
- 2.4 The Policy applies to all hardware provided by Barrett-Bell Ltd and also covers company hardware and private hardware in use whilst on Barrett-Bell Ltd's premises and connected to the Barrett-Bell Ltd network or representing Barrett-Bell Ltd off-site.
- 2.5 This Policy should be read in conjunction with the Acceptable ICT Usage Policy for Learners.

3 IT Areas of Concern

3.1 The following sections cover the main ICT areas:

- Company Access (individual's responsibility)
- Company Security
- Unacceptable and Unlawful Actions
- Exceptions to Conditions of Use
- Clear Desk and Clear Screen Policy (good housekeeping)
- Working Off-site (laptop safety)
- Mobile Storage Devices (secure data)
- Software (licences)
- Viruses (detection)
- Telephony Voice Equipment (conditions of use)
- Monitoring and Filtering (process)
- Cessation of Contract (actions)

3.2 **Company Access (individual's responsibility)** – Staff will only be given permission to access the system when they have undertaken the following safeguards:

- Access to the Barrett-Bell Ltd IT systems is controlled by the use of **User IDs and passwords**. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions when using the Barrett-Bell Ltd's IT system(s)
- Staff must not allow anyone else to use their user ID and password on any Barrett-Bell Ltd IT system even on a temporary basis
- Staff must not use someone else's user ID and password to access Barrett-Bell Ltd's IT system, including searching the Internet or sending emails
- Passwords must be changed at regular intervals and all passwords must involve a range of capital and lower-case letters/numerals/special symbols to aid password security. The day-to-day security of hardware and software is the responsibility of the individual
- Acceptance of this Policy has been completed and returned (the Appendix I Form must be signed/dated by the employee and countersigned by HR Staff or Directors during Induction or after any updates)

3.3 **Company Security** – Staff are requested to ensure they follow the regulations and must not:

- Leave their password unprotected, by writing it down or keeping the same password for long periods of time
- Leave their user accounts logged in but unattended and/or unlocked at any time on the computer

- Exceed the limits of their authorisation or specific business need to interrogate the system or data (Line Managers will allocate each of their Staff the limits of their rights to access of the IT and data withing Barrett-Bell Ltd
- Connect any non-Barrett-Bell Ltd authorised device to the Barrett-Bell Ltd network or IT systems
- Connect Barrett-Bell Ltd devices to the Internet using non-standard connections
- Break the regulations which regulate the lawful use of software packages and the licences attached to software
- Perform any unauthorised actions that could modify the Barrett-Bell Ltd's IT system, which intentionally or recklessly introduces any form of spyware, malware, computer virus or other potentially malicious software on the system or compromise data protection regulations
- Make official commitments or purchases of packages/licences through the Internet or email on behalf of Barrett-Bell Ltd unless authorised to do so
- Download any software from the Internet without prior approval of the IT Support and/or Directors to ensure that no malware is installed or licence agreements broken
- Introduce any data-interception, password-detecting or similar software or devices to the company network or attempt to carry out any hacking activities
- Store Barrett-Bell Ltd data on any non-authorised Barrett-Bell Ltd equipment or not adhere to GDPR/data protection regulations regarding stored data
- Place any information on the Internet that relates to Barrett-Bell Ltd, alter any information about it, or express any opinion about Barrett-Bell Ltd, unless they are specifically authorised to do this
- Send unprotected sensitive or confidential information externally
- Give access to and/or transfer Barrett-Bell Ltd data or software to any person or organisation outside Barrett-Bell Ltd without the written permission and authority of Barrett-Bell Ltd
- Forward Barrett-Bell Ltd mail or documents to personal non-Barrett-Bell Ltd email accounts (eg. a personal Hotmail account)
- Misuse the IT and its capability or encourage anyone else to do so, including on their behalf

3.4 **Unacceptable and Unlawful Actions** - Individuals must not (subject to any exemptions defined by Barrett-Bell Ltd) access IT directly or indirectly for the viewing, download, creation, manipulation, transmission or storage of unacceptable material which includes:

- Use of material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation or any protected characteristic

- Use of unlawful material or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others or incite criminal behaviour
- Use of material which is subsequently used to facilitate harassment, bullying and/or victimisation of another person(s)
- Use of profanity, obscenities or derogatory remarks in any communications
- Access, downloading, sending or receiving any data including images, which Barrett-Bell Ltd considers offensive in any way, including sexually explicit, misogynistic, discriminatory, defamatory, libellous or which advocates or promotes any unlawful act
- Access offensive or potentially offensive, obscene or indecent images, data or other material, or use any data (including by use of AI) to manipulate into obscene or indecent images or material
- Use the Internet or email to gamble, view pornography, enter adult chat rooms, visit the Dark Web, troll others and make nuisance communications or undertake any other activity that may bring the company into disrepute or lead to criminal allegations or loss of company reputation
- Access any material with the intent to defraud or to deceive a third party
- Use the Internet or email for personal gain, to conduct a personal business or be involved in the pursuance of commercial activities that are not in the interests of Barrett-Bell Ltd
- Download copyrighted material such as music media MP3 files, film and video files, rights to trademarks without appropriate approval that may infringe the copyright, intellectual property rights, privacy rights of a third party or that is in breach of a legal duty owed to another party
- Use the IT system in a way that could affect its functionality, reliability or effectiveness (eg. by denying access to the system by other users, intentionally or accidentally wasting Staff/Learner time or company resources, disrupting the work of other users, or corrupting, altering or destroying colleague's/Learner data without their consent or distributing chain letters, spam or malware that reduces performance and productivity)

3.5 Exceptions and Exemptions to Conditions of Use – Under normal circumstances 3.2 – 3.4 must be adhered to and failure to do so may result in disciplinary measures. There are, however, instances when certain exemptions may pertain:

- The use of the Barrett-Bell Ltd's Internet and email is intended solely for business use. With the Director's express permission some personal use is permitted where such use does not affect the individual's business performance, is not detrimental to Barrett-Bell Ltd in any way, is not in breach of any term and condition of employment and does not place the individual or Barrett-Bell Ltd in breach of statutory or other legal obligations

- Permission must be sought prior to any personal use and written agreement obtained before any personal use
- There are a number of curriculum activities that could be considered unacceptable use, as defined above (3.3) – eg. research into what constitutes discriminatory or threatening material, material for the sole purposes of training for Safeguarding or the Prevent Duty or research into computer intrusion techniques to enhance administration security. Senior Staff must be notified if any member of Staff is contemplating access these sites for curriculum or training purposes prior to accessing sites.
- Any materials that could be misconstrued as suspect must be isolated and removed asap after the training/research session
- All individuals are personally accountable for their actions on the Internet and email systems

3.6 Clear Desk and Clear Screen Policy (good housekeeping) - in order to reduce the risk of unauthorised access or loss of information, Barrett-Bell Ltd enforces a clear desk and screen policy as follows:

- Personal, sensitive or confidential business information must be protected using security features provided (e.g. complex passwords, secure print on printers, not sharing unlocked computers)
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended
- Care must be taken to not leave confidential or company sensitive materials on desks, pinned on wall post-it notes, printers or photocopiers
- All business-related printed matter must be kept securely locked away and disposed of using confidential waste bins or shredders when appropriate

3.7 Working Off-site (laptop/device safety) - it is accepted that laptops and mobile devices may be required to be taken off-site. The following controls must be applied:

- Working away from the office must be in line with Barrett-Bell Ltd Remote Working Policy and best practice
- Laptops must be carried as hand luggage when travelling and kept in personal possession at all times
- Equipment and media taken off-site must not be left unattended in public places and not left visibly in sight in a car. No laptop or phone should left in the boot of a vehicle overnight
- Information should be protected against loss or compromise when working remotely for example at home, off site or in public places. Laptop encryption must be used
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a secure password and/or a PIN, Multi-Factor Authentication and, where available, encryption and passkeys
- If any laptop/phone etc is lost – this must be reported to the Directors immediately and a list of all sensitive data be provided to the Directors. The

equipment must be blocked asap and any 'find' devices used to locate the missing items

3.8 Mobile Storage Devices (secure data) – it is sometimes easier to lose small transportable storage items than larger equipment, hence:

- Mobile devices such as USB memory sticks, SSD storage, flash drives, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data
- Only Barrett-Bell Ltd authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data
- Use of mobile storage devices must be kept safe and within sight at all times
- All data protection and GDPR regulations must be adhered to at all times
- Any data loss or data corruption must be reported to the Directors immediately

3.9 Software (licences) - Staff must use only software that is authorised by Barrett-Bell Ltd on Barrett- Bell Ltd's computer systems and hardware:

- Authorised software must be used in accordance with the software supplier's licensing agreements and limitations
- Do not share software with any other person as breaking licence agreements can lead to legal action and fines
- All software on Barrett-Bell Ltd computers must be approved and installed by the Barrett-Bell Ltd IT department
- Individuals must not store personal files such as music, video, photographs or games on Barrett-Bell Ltd IT equipment

3.10 Anti-virus (detection) - all PCs/laptops have antivirus software installed to detect and remove any virus automatically. If in any doubt, please have your laptop scanned for viruses and malware by the IT Support. Individuals must not:

- Remove, amend or disable anti-virus software
- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved Barrett-Bell Ltd anti-virus software and procedures
- Attempt to install alternative virus detection programmes on IT equipment
- Share documents or forward emails when a virus has been identified
- All viruses and malware must be reported immediately to the Directors

3.11 Telephony Voice Equipment (conditions of use) – the use of Barrett-Bell Ltd voice equipment (land line, answerphone) is intended for business use only. Staff should follow these rules:

- When/if answering the phone Staff should never impersonate any other person when making or receiving calls – please take a number and name and say they will be phoned back

- Staff must not clear or wipe any answerphone messages unless they are designated to do this and have written the details down accurately
- Staff must not accept reverse charge calls from domestic or international operators, unless it is for Barrett-Bell Ltd business use and the member of Staff is cleared to accept reverse charges
- Staff must not use Barrett-Bell Ltd's voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances as agreed by the Directors
- Staff must not use Barrett-Bell Ltd's voice equipment for conducting private business
- Staff must not use Barrett-Bell Ltd's voice equipment to make nuisance, hoax or threatening calls to internal or external destinations
- All non-urgent personal communications should be made at an individual's own expense using alternative means of communications and in their own time (i.e. at break, lunch or after the end of the day)
- Personal phones should only be used to show Learners specific learning content or to make/receive personal calls.
- Use of mobile phones to make or receive personal calls must limit these to their own non-teaching time and Staff must set a good role model in relation to the use of mobile phones

3.12 **Monitoring and Filtering (process)** - All data that is created and stored on Barrett-Bell Ltd computers remains the property of Barrett-Bell Ltd and there is no official provision for individual data privacy, however, wherever possible Barrett-Bell Ltd will avoid opening personal emails but retains the right to do so. (NB. Personal emails should be kept separate from company emails.)

- All suspected breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with Barrett-Bell Ltd Disciplinary Procedures. Serious breaches that involve Safeguarding issues may be passed onto other services such as the Information Commissioners Office (ICO), Police, Social Services and/or LADO as appropriate.
- IT system logging will take place where appropriate and investigations will be commenced where reasonable suspicion exists of a breach of this or any other company Policy.
- Barrett-Bell Ltd has the right under certain conditions to monitor activity on its systems, including Internet and email use, in order to ensure systems security and effective operation, to investigate breaches of the Policy and to protect against misuse and ensure robust Safeguarding.
- Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 2018, the Regulation of Investigatory Powers Act amended 2016 and the Telecommunications Lawful Business Practice Interception of Communications Regulations 2000.

- It is everyone's responsibility to report suspected breaches of the Acceptable ICT Usage Policy without delay to the Line Manager, the IT support helpdesk and/or the Directors.
- This Policy must be read in conjunction with the Computer Misuse Act updated 2015, Data Protection Act (GDPR implementation) 2018 and Single Equalities Plan.

3.13 Cessation of Contract (actions) – when Staff leave Barrett-Bell Ltd they must:

- Return all Barrett-Bell Ltd all equipment (eg. laptops and mobile devices)
- Return all data, including USB memory devices and mobile data devices
- Identify any data that the company needs to dispose of in order to meet Data Protection requirements (please do not delete or shred data unless directed to do so – the company will undertake this function)
- Ensure all personal information (photos, vids, music) and removed and clear the search engine history and empty the desktop bin
- All Barrett-Bell Ltd data or intellectual property developed or gained during the period of employment remains the property of Barrett-Bell Ltd and must not be retained beyond termination or reused for any other purpose (NB. theft of intellectual property is a crime and will be reported as such)

Appx I. Acceptance of the Policy

Please make sure that you have read, understood and accepted this Barrett-Bell Ltd Acceptable Internet Usage Policy before you sign this document.

Any Breaches of this Policy could result in withdrawal of access to the IT or disciplinary actions.

By signing you are committing to comply with these guidelines.

I confirm that I have read, understood and will adhere to the terms and requirements of this Acceptable Internet Usage Policy:

Employee Name (print)	
Employee signature	
Date employee signed	
HR/Directors' signature	
Date HR/Director signed	

