Instituid Bhreisoideachais
na Carraige Duibhe

Blackrock Further
Education Institute

Information and Communications Technology Usage Policy

March 2022

Contents

1 General

The purpose of this policy is to outline the acceptable use of BFEI's Information and Communication Technology (ICT) resources. This policy is intended to protect staff, students and the Institute.

This policy applies to all users of BFEI's ICT resources including staff, students, visitors and other external contractors whether these resources are used on premises in BFEI or remotely.

ICT resources are provided by BFEI in conjunction with DDLETB (Dublin and Dún Laoghaire Education and Training Board), ETBI (Education and Training Boards Ireland) and HEAnet.

ICT resources include (but are not limited to):

- Desktop and laptop computers in classrooms, staff offices and on loan to staff and students.
- Audio Visual equipment in classrooms, staff offices and on loan to staff and students.
- Printers and photocopiers
- Network infrastructure including cabling, WiFi Access Points, routers, switches and firewalls
- Servers
- Software
- Online services, including Microsoft365, Moodle, Adobe Creative Cloud and other online services
- Internet connection.

Users are required to use ICT equipment and resources for academic purposes in a safe, respectful and legally compliant manner. Inappropriate use exposes the Institute to threats including malicious attacks, compromise of systems and services, and legal actions.

All computer and data resources provided by BFEI are the property of BFEI and not the personal property of individual users.

All software which is provided by BFEI is licensed by BFEI for use by current BFEI learners and staff and may not be downloaded, stored or transferred for use by any other party. Software should not be downloaded from the Internet or installed from any other source and used on BFEI devices without the permission of the ICT Department.

BFEI data must be stored on devices owned and managed by BFEI. All BFEI devices for use anywhere outside of the campus, must enforce encryption on all data such that it is only accessible by BFEI staff. Remote access to BFEI data is provided only through Microsoft 365 and must be accessed only using a BFEI approved app.

2 Data Privacy and Monitoring

BFEI reserves the right to maintain audit and activity logs and to monitor the use of its ICT resources for the following purposes:

- Maintaining the availability and performance of ICT resources
- Detecting, preventing, and investigating ICT security-related incidents
- Responding to legal or compliance requests
- Complying with any legal and statutory obligations
- Investigating and enforcing BFEI Policies and Codes of Conduct

Users who have access to or are responsible for the personal data of other users stored on BFEI's ICT equipment must ensure that access to and use of the data complies with DDLETB's Data Protection policy and the provisions of GDPR (General Data Protection Regulations).

3 Malfunction

Before a user starts using a device s/he should check:

- that the device is in full working order and not defaced or damaged
- that no other user is logged into the device

Malfunctions should be reported immediately to fixit@bfei.ie. Any malware, security error/warning messages or security incidents must be reported promptly by taking a screen shot of the message and emailing fixit@bfei.ie. **The original message/s should not be forwarded.**

When finished using a device, **users must log-out** and leave the device ready for other users. Failing to log out creates an unacceptable security risk.

4 Use of IT Resources

ICT resources are provided to support teaching, learning and administrative activities. Users are provided with accounts to permit access to ICT resources. These include, but are not limited to:

- Office 365
- Email
- Microsoft Teams
- OneDrive
- Moodle
- Adobe
- BFEI server accounts
- Printing

Users will receive a Microsoft 365 account. Users will be issued with usernames and passwords. Passwords protect the identity of each user. Passwords must remain confidential to each user and must not be relayed to any other person. Users must not utilise any other person's identity, attempt to exceed their assigned access rights or attempt to gain access to another user's resources or data. Users must not attempt to bypass or probe any security mechanisms governing access to the computer systems. Users must not misrepresent themselves as other individuals: this includes using another user's identity.

The Microsoft 365 account includes an @bfei.ie email address and access to the Microsoft Office suite of applications including Word, Excel and PowerPoint.

This email address:

- should be checked by users **every working day**
- will be the **ONLY** email address used by teaching staff to communicate with students once classes commence. Personal email addresses will not be used.
- Email communication between BFEI users must not contain remarks and/or images which are abusive, obscene, threatening, defamatory, offensive, discriminatory or harassing
- Email distribution lists may only be used by teaching staff in connection with BFEI business.

BFEI retains ownership of all accounts, data, and services for all accounts. Users are responsible for all activities and information accessed using their identity. Users must ensure, in so far as is practicable, that use conforms with BFEI's policies.

Users must not undertake or facilitate activity that could jeopardise in any way, the security (confidentiality and integrity), availability and performance of ICT resources, or compromise their utility or availability to other users.

Users must not:

- Steal or maliciously damage BFEI hardware or software
- Interfere with files, system settings, network wiring, computer hardware or peripherals
- Seek to access unauthorised areas of the Institute's ICT resources
- Install unauthorised software
- Interfere with or disable the Endpoint Protection (anti-virus and firewall) software installed on devices
- Access, download, print, save, create or transmit any abusive, obscene, threatening, defamatory, offensive, discriminatory or harassing images or material
- Drink (except for bottled water), eat or chew gum while using computing resources
- Use BFEI resources for commercial purposes
- Apply make-up in computer labs

BFEI's ICT resources must not be used to:

- Advocate or promote any unlawful act
- Harass, bully, discriminate or victimise others and/or cause harm, offence, nuisance, or needless anxiety to others
- Corrupt, destroy or disrupt other users' data or deny and disrupt services to other users, for example by sending unnecessary or trivial messages, chain, junk mail or unsolicited bulk or marketing email (spam)
- Publish or transmit anything that is libellous, defamatory or incites hatred
- Access, display or print pornographic or other offensive material

- Plagiarise or infringe the copyright, licence terms, trademark or proprietary rights of another person or organisation
- Deliberately misrepresent their personal views as those of BFEI or any other person or organisation
- Disrupt the work of other users

5 Data Retention including Saving/Backing Up Work

Users are provided with Microsoft 365 accounts, which includes online storage. **Users are responsible for backing up their own data.** Users should ensure that data stored on a local computer is either backed up automatically (synced to **OneDrive)** or backed up manually to **OneDrive**. Computers may be removed from or relocated within rooms without prior notice.

BFEI student accounts and the data they contain are deleted at the end of each academic year. Deleted accounts include (but are not limited to) Microsoft 365, email, Moodle, Microsoft Teams, Adobe, OneDrive, SharePoint, printing and BFEI Windows accounts. Before the end of the academic year each student should remove any data associated with their account(s). Each student should back up the data they wish to retain to a suitable storage location separate to their BFEI account(s).

USB Memory/flash drives are NOT permitted on staff PCs.

Staff accounts are archived 30 days after the date of departure from BFEI.

All computers and laptops in classrooms and staff offices are erased and rebuilt at the end of each academic year.

6 Access to IT Rooms After Hours and During Holidays

Outside formal instruction hours (after hours and holiday times)

a) Students must sign the attendance register (located at the caretakers’ office) indicating time in and time out and the computer room being used.

b) The room must be temporarily vacated if requested by BFEI staff.

7 Equipment on Loan

Staff and students who borrow ICT equipment are required to sign an *Equipment Loan Agreement* Form and comply with this policy.

8 Bring Your Own Device

Users who use their own devices in BFEI are required to comply with this policy. These devices should be appropriately secured with Endpoint Protection (anti-virus and firewall) software.

9 Remote Teaching and Learning

If required, remote teaching and learning will be facilitated using Microsoft Teams which is provided as part of the Microsoft 365 account.

10 Support

The *Student IT Induction Handbook* provides detailed instructions on how to access and use the systems and platforms provided by BFEI.

Users can also request support for ICT issues by emailing fixit@bfei.ie.

BFEI courses are delivered using Microsoft Windows devices. Other operating systems such as MacOS or Chrome OS are not used and cannot be supported.

11 Reporting Requirements

Users are required to report the following to fixit@bfei.ie:

- Equipment malfunctions and other ICT issues
- Virus warnings/messages or security incidents
- Suspected abuse of ICT resources
- Suspected breaches of GDPR
- Messages/images/content that is abusive, obscene, threatening, defamatory, offensive, discriminatory or harassing

12 Breaches of Policy

Any breach of this policy may result in disciplinary action under the Institute's Policies and Procedures including the Code of Conduct as well as referral to An Garda Síochána or other regulatory bodies