English Speaking Board (International) Ltd.
IT Acceptable Usage Policy

Contents

1. Policy Introduction

This policy provides clear and concise information on the acceptable use of IT facilities by employees, Trustees, third parties and contractors providing services on behalf of English Speaking Board (International) Ltd. (ESB International).

1.1 Purpose of the IT Acceptable Usage Policy

The purpose of the IT Acceptable Usage Policy (the Policy) is to define the acceptable use of ESB's IT facilities, including the 'MyESB' Hub, Egnyte, third party platforms (e.g. Cirrus, Canvas, AST), ESB SharePoint Resources, email, social media and internet resources. Whether this is via laptops, PCs, tablets, mobile phones and other mobile devices, in order to preserve the integrity, availability and, where appropriate, confidentiality of ESB International information and information systems, ensuring any form of communication, using technology, that an individual will use in their role is used appropriately and in line with GDPR regulations.

The Policy establishes a framework within which users of these facilities can apply self-regulation to their use. The guidance is intended to support the use of ESB International's IT facilities.

The Policy describes the standards that users are expected to observe and ensures that users are aware of the legal consequences attached to inappropriate use of the facilities. The Policy informs users that the use of ESB International's IT facilities for all purposes may be monitored and, in some cases, recorded. Usage of facilities in breach of the Policy may lead to action being taken.

1.2 Scope of the Policy

This Policy applies to the use of any IT facilities, provided by English Speaking Board (International) Ltd. (ESB International). This includes internet access and email services, hardware (i.e. PCs, laptops and peripherals), software (i.e. Microsoft Office) and web-based services (e.g.. Office 365, SharePoint, Egnyte, the 'MyESB' Hub and ESB Database).
The Policy will be distributed to users of any of ESB International's IT facilities and has to be strictly adhered to by them.

1.3 Appropriate and Proper Use

ESB International promotes the appropriate and proper use of all IT facilities (including, but not limited to, those in the scope of the policy), which the company provides for its staff or other authorised users in pursuance of its business. The purpose of this policy is to protect both the user and ESB International. Inappropriate use of ESB's IT facilities exposes ESB International to risks including virus attacks, compromise of systems and services, and legal issues.

1.4 Regulatory Framework

Associated with the provision of these facilities and services, ESB International has a responsibility to provide a suitable regulatory framework, including specific standards and guidance for the appropriate use of these ESB International facilities and services. The Policy constitutes a component part of this regulatory framework.

ESB International is a registered charity regulated by The Charity Commission and is committed to ensure that all charity assets are safe, properly used and accounted for.

As an awarding organisation, ESB International is regulated by the following Regulators: Ofqual (England), CCEA Regulation (Northern Ireland) and Qualifications Wales (Wales). ESB International is committed to comply with its regulatory requirements in line with the following:

Ofqual Handbook – General Conditions of Recognition (2017 updated May 2022):

- Condition A4, employees and contractors must ensure that they comply with the Conflict of Interest Policy and dutifully inform ESB International of any known conflicts for registration onto the ESB Database.
- Condition A5.1, capacity to undertake the delivery of qualifications which we make available.
- Condition A5.2, arrangements which will ensure that sufficient technical equipment and support is available at all times.

CCEA General Conditions of Recognition (April 2019):

- Condition A5, availability of adequate resources and arrangements.

Qualifications Wales – Standard Conditions of Recognition (October 2018):

- Condition A5, availability of adequate resources and arrangements (5.1 and 5.2 in particular).

ESB International and its employees must also adhere to the Data Protection Act (2018) and UK GDPR Regulations. For further information please see our Data Protection Policy available on our website.

1.5 Monitoring Arrangements

ESB International will maintain appropriate monitoring arrangements in relation to all IT facilities that it provides, to ensure compliance with both policy and regulation. These monitoring arrangements will operate on a continual basis and will apply to all users, as permitted by The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

1.6 Policy Review

The Policy will be reviewed and, if necessary, amended from time-to-time, with particular regard to the expected developments in the operational use of the system and by reference to the development of recognised best practice. There will also be periodic re-issues of the Policy, supported by sign-up acceptance by users of the facilities.

2. Regulations

2.1 Acceptable Use

ESB International provides IT facilities & Services for use in connection with approved business activities of the company. Any suspected security breach (e.g. virus infection, unexplained data loss or data corruption, hardware theft or loss, misuse of user account, unauthorised data access, data or email with offensive content etc.) shall be reported immediately to IT Support, in order that immediate response activities can be launched.

2.2 Bring Your Own Device Policy (B.Y.O.D.)

ESB International operates Bring Your Own Device Policy (B.Y.O.D.). The purpose of the B.Y.O.D. Policy is to provide guidelines on the appropriate usage of personal devices used for any data, documentation, email correspondence and audio-visual materials relating to ESB International's business. All users must understand that whenever a computer device is connected to the organisation's network, systems or computers, opportunities exist for:

- Introducing viruses, spyware, or other malware.
- Purposefully or inadvertently copying sensitive and/or proprietary organisation information to unauthorised devices.
- Loss of data that may adversely affect the organisation if it falls into the wrong hands.

As a result of any of these circumstances, a user connecting their own device to ESB International's resources, systems, or networks could interrupt business operations, cause unplanned downtime for multiple users, and/or cause a data breach releasing organisation, client, and/or partner data to unauthorised parties. In worst-case scenarios (and in events entirely realised at other organisations), civil and criminal penalties for the user and/or substantial costs and expenses to the organisation could arise.

2.2.1 Acceptable usage (B.Y.O.D.)

All employees and contractors must ensure that they have the relevant and appropriate equipment to ensure the safety of company resources and data, this is outlined in the minimum device requirements section of this document. The use of a personal device is permitted to perform/assist in the delivery of ESB International's work, given that proper care is given, and protocols are followed to ensure that company data is not compromised.

2.2.2 Inappropriate usage (B.Y.O.D.)

Inappropriate usage of a device under B.Y.O.D. is caused by intentional, poor care and negligence when using personal equipment that would pose a risk to the organisation's data and computing resources. ESB International employees and contractors must ensure that any data stored on a personal device is kept safe and separate from any personal documentation. The use of a device, which is also used for alternate business purposes that directly conflict with ESB International's interests, is strictly prohibited. The intentional introduction of viruses, spyware or malware or the purposeful spread of sensitive information/ESB International organisation information would be a direct breach of the B.Y.O.D. Policy and would be subject to authoritative action.

2.2.3 Minimum Device requirements (B.Y.O.D.)

In accordance with the B.Y.O.D. Policy the hardware and software requirements are the minimum required by a device to be used for business purposes. These are: -
Operating system requirements:

- Windows: Windows 7 and above (Including windows 7, 8 & 10).
- Mac: Mac OS X 10.6 Snow Leopard (Released in 2008).

Anti-Virus/Anti Malware protection:
The device must have an anti-virus/anti-malware program installed that is performing frequent scans to ensure device security.

Browser requirements:
The 'MyESB' Hub is designed to work with most web 2.0 websites and is backwards compatible however, we advise using standard browsers for best results. These are: -

- Microsoft Edge
- Google Chrome
- Mozilla Firefox
- Safari (Version 10+)

Mobile Devices:

- Apple Devices: IOS 13+
- Android devices: Android Pie version 9.0 and above (Released in 2018)

Devices which do not meet the minimum requirements are in breach of the B.Y.O.D. Policy as they would be more susceptible to viruses.

2.3 Egnyte

Egnyte is utilised by ESB International as its cloud storage facility for data. All employees, Trustees, third parties and contractors must ensure they store all ESB International data within the Egnyte file structure. All users must download the file sync software as outlined in the ESB-SOP-16 ESB Egnyte User Guide document. The full sync software must be used and all ESB International data must be stored within the shared folder location the user has access to, doing this ensures that company data is always available and in a safe location. Saving ESB International data in any other location is not permitted under any circumstances. Upon a member of staff leaving ESB International, HR will inform IT through the helpdesk of the user and permissions that require removal. IT will then perform and confirm the action through the helpdesk function.

Video & Audio Files of learners' assessments will be stored on Egnyte for 6 months. After 6 months the files will be deleted by IT. This process will only happen when QA raise a ticket to inform IT that the data is ready to be deleted, once the task is complete IT will update QA who will in turn inform the client of the deletion.

2.4 MS Teams

Any data downloaded from MS Teams meetings will be the responsibility of the individual to remove from their device during their monthly data audit.

2.5 We Transfer

All employees, third parties or contractors who have a need to send any personal data outside of ESB International (to clients, suppliers etc.) must use We Transfer to send the information. Personal data must not be sent via email as this is not a safe transaction, WeTransfer provides a safe (encrypted) transfer of data. A WeTransfer account is free to setup and can be done here https://wetransfer.com/

2.6 General Standards of Use and Ownership

While ESB International aims to provide a reasonable level of privacy, users must be aware that any data produced for ESB International and its customers, whether using their own facilities or ESB's IT facilities, remains the property of ESB International.

All users dealing with personal data must comply with current Data Protection Law which is outlined in ESB International's Data Protection Policy available on our website www.esbuk.org.

IT facilities provided by ESB International must not be used: -

a. Under any circumstances for any activity that is against the law
b. For the creation, storage or transmission of
    i. Any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material
    ii. Material with sexual, racist, discriminating, or any other content that is in violation of sexual harassment or hostile workplace laws
    iii. Material which is designed or likely to cause annoyance, inconvenience or needless anxiety
    iv. Defamatory material
    v. Material that includes false claims of a deceptive nature
c. For so-called 'flaming' i.e. the use of impolite terms or language, including offensive or condescending terms.
d. For activities that violate the privacy or security of other users (e.g. by accessing data of which the user is not an intended recipient, unless within the scope of regular duties).

e. For criticising individuals, including copy distribution to other individuals.
f. For publishing to others the text of messages written on a one-to-one basis, without the prior express consent of the author.
g. For the creation or transmission of anonymous messages, i.e. without clear identification of the sender.
h. For installation, distribution, procurement, storage or transmission of 'pirated' or other illegal software products. The same applies to any other copyrighted material.
i. For the creation, procurement, storage or transmission of material which brings ESB International into disrepute.

2.7 Acceptable email use Policy

Use of email by ESB International employees, Trustees and ESB International contractors is permitted and encouraged where such use supports the goals and objectives of the business.

The purpose of the email use policy is to safeguard employees and contractors by outlining usage that would be deemed unacceptable and/or detrimental to the business.

Employees and contractors must ensure that they: -

- Comply with current legislation
- Use email in an acceptable and appropriate manner
- Do not create unnecessary business risk to the company by their misuse of the email facilities.

2.8 Inappropriate behaviour

The following behaviour by an employee, Trustee or contractor is considered inappropriate:

- Use of company communications systems to set up personal businesses or send chain letters
- Forwarding of company confidential messages to external locations
- Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal, discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment.
- Accessing copyrighted information in a way that violates the copyright
- Breaking into the company's or another organisation's system or unauthorised use of a password/mailbox
- Broadcasting unsolicited personal views on social, political, religious or other non-business related matters
- Transmitting unsolicited commercial or advertising material
- Undertaking deliberate activities that waste staff effort or networked resources
- Introducing any form of computer virus or malware into the corporate network

2.9 Preventing the Spread of Malicious Software (Viruses)

Users of ESB IT facilities must take all reasonable steps to prevent the receipt and transmission of malicious software e.g. computer viruses; Trojans; malware; spyware.

Users must not introduce malicious programs onto ESB International equipment (e.g. viruses, worms, Trojan horses, email bombs, etc.). If you receive a potentially malicious file via any medium whilst using ESB's IT facilities (including email), or suspect that a file you've received is malicious, you must inform IT Support as soon as possible and under no circumstances attempt to open the file.

2.10 Monitoring

ESB International employees and contractors are subject to device audits and monitoring requests from the ESB IT Team to ensure that the device is in-line with the ESB International hardware and software requirements. The purpose of these requests is to ensure that the devices are fit for purpose whilst also ensuring that the individual's information is safe and the device is secure. ESB International facilities such as email, SharePoint, Egnyte and the ESB Database are provided for business purposes, therefore, the company maintains the right to examine these resources and inspect any data recorded.

All employees are required to self audit their devices every 3 months and remove all files and emails containing personal data.

2.11 Legal Consequences of Misuse of IT Facilities

In most cases involving the civil or criminal law, files, records and electronic/internet-based communications of many kinds (deleted or otherwise) are produced as evidence in a permanent written form.

There are several areas of law which apply to the use of IT facilities and services and which could involve liability of users or the company. These include the following: -

a. **Intellectual Property**. Anyone who uses email to send or receive any materials that infringe the Intellectual Property Rights of a third party may be liable to that third party, if such use is not authorised by them.
b. **Obscenity**. A criminal offence is committed if a person publishes any material which is pornographic, excessively violent or which comes under the provisions of the Obscene Publications Act 1959. Similarly, the Protection of Children Act 1978 makes it an offence to publish or distribute obscene material of a child.
c. **Defamation**. As a form of publication, the Internet is within the scope of legislation relating to libel where a statement or opinion is published which adversely affects the reputation of a person, group of people or an organisation. Legal responsibility for the transmission of any defamatory, obscene or rude remarks which discredit an identifiable individual or organisation will rest mainly with the sender of the email and may lead to substantial financial penalties being imposed.
d. **Data Protection**. Processing information (including photographs) containing personal data about individuals requires the express written consent of those individuals. Any use of personal data, beyond that registered with the Data Protection Commissioner or which does not fall in line with GDPR compliance, will be regarded as an illegal act.
e. **Discrimination**. Any material disseminated, which is discriminatory or encourages discrimination may be unlawful e.g. where it involves discrimination on the grounds of sex, race, age or disability.

The above is only designed to be a brief outline of some of the legal consequences of misuse of IT facilities.

Revision No	Change to previous release	Reason for change
1	New release	N/A
2	SQA reference removed on p2	Withdrawal from SQA Accreditation
3	Egnyte, WeTransfer and MS Teams software information added in point 2 reference added to charity commission and data protection policy, self audit requirements added in 2.10	