BEC
TEACHER
TRAINING

Email and Internet policy for staff and trainees

This section is organised as follows:

This policy sets out BEC Teacher Training's (BECTT's) expectations of staff and other users (working for or on behalf of BECTT), in respect to the use of email and access to the Internet (the expectations also apply to the use of the secure website) via BECTT Internet facility or computer equipment. This policy applies to all electronic mail systems and services provided by the BECTT, all users and holders and uses of BECTT's and Internet services.

This policy is designed to express BECTT's philosophy with regard to electronic communication and to set forth general principles that employees, trainees, schools and staff would apply when using electronic media and services. This guidance does not attempt to cover every possible situation.

1. Introduction

E-mail and the Internet can be extremely valuable tools in an educational context, encouraging the development of communication skills, and transforming the learning process by opening up possibilities that, conventionally, would be impossible to achieve. BECTT encourages the use of electronic mail as a medium for paper mail replacement and as a means of enhancing communications.

2. Objectives

The objective of this policy is to ensure that:

- BECTT is informed about the applicability of policies and laws to electronic mail and Internet usage.
- Electronic mail services and the Internet are used in compliance with those policies and laws.
- Users of electronic mail services are informed about how concepts of privacy and security apply to electronic mail; and
- Disruptions to BECTT mail and other services and activities are minimised.

3. Usage

Those that use BECTT electronic mail services and/or the Internet are expected to do so responsibly, comply with all applicable laws, other policies and procedures of BECTT and with normal standards of professional and personal courtesy and conduct. Appendix 1 provides an illustration of good email practice.

4. Security

BECTT follows sound professional practices to secure e-mail records, data and system programmes under its control. As with standard paper based mail systems, confidentiality of e-mail cannot be 100% assured. Consequently users should consider the risks when transmitting highly confidential or sensitive information and use the appropriate level of security measure.

Enhancement of the base level security to a higher or intermediate level can be achieved by the use of passwords for confidential files. It should be remembered e-mails forwarded from another individual can be amended by the forwarder. This possibility should be considered before acting on any such mail.

In order to effectively manage the e-mail system the following should be adhered to:

- Open mailboxes must not be left unattended.
- Care should be taken about the content of an e-mail as it has the same standing as a memo or letter. Both the individual who sent the message and/or BECTT can be sued for libel.
- Reporting immediately to Xanda when a virus is suspected in an email.

5. Misuse & prohibited communications

Electronic media must not be used for knowingly viewing, transmitting, retrieving, or storing any communication that is:

- Discriminatory or harassing
- Derogatory to any individual or group
- Obscene or pornographic
- Defamatory or threatening
- Engaged in any purpose that is illegal or contrary to BECTT's policy or business interests.

Further, all forms of chain mail are unacceptable and the transmission of user name, passwords or other information related to the security of BECTT's computers is not permitted.

Except in cases in which explicit authorisation has been granted by BECTT management, employees and trainees are prohibited from engaging in, or attempting to engage in:

- Monitoring or intercepting the files or electronic communications of other employees, trainees or third parties.

- Hacking or obtaining access to systems or accounts they are not authorised to use.
- Using other people's log-ins or passwords.
- Breaching, testing, or monitoring computer or network security measures.
- E-mail or other electronic communication that attempts to hide the identity of the sender or represent the sender as someone else.
- Using electronic media and services must not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.
- Anyone obtaining electronic access to other companies' or individuals' materials must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

BECTT policy prohibit the theft or abuse of computing resources. This applies to e-mail and Internet services and includes:

- Unauthorised entry.
- Use, transfer and tampering with other people's accounts and files.
- Interfering with other people's work or computing facilities.
- Sending, storing or printing offensive or obscene material including content that may be interpreted as sexual or racial harassment.
- Mass mailing of personal messages.
- Internet use for personal messages.
- Internet use for personal commercial purposes.
- Using the Internet/secure website facilities or equipment to deliberately propagate any virus, worm, Trojan horse or any such other programme that is harmful to normal computer operations.
- Accessing any obscene or pornographic sites. Sexually explicit material may not be viewed, archived, stored, distributed, edited or recorded using BECTT's networks or computing resources.

If a user finds himself/herself connected accidentally to a site that contains sexually explicit or offensive material, they must disconnect from that site immediately. Such unintentional access to inappropriate Internet sites must be reported immediately to the Executive Director. Any failure to report such access may result in disciplinary action.

It is impossible to define all possible unauthorised used, however, disciplinary action may be taken where an employee's actions warrants it. Other actions deemed unacceptable, although not exhaustive, include:

- Theft or copying of files without permission.
- Sending or posting BECTT's confidential files outside of the organisation or inside the organisation to unauthorised staff.
- Refusing to co-operate with reasonable security investigation.

6. Personal use

The email system and the Internet are business tools provided to staff and other users at a cost. Hence, it is expected that this resource will be used primarily for the business/course related purposes.

BECTT e-mail and Internet service may be used for incidental personal purposes, with the approval of the Executive Director, provided that it does not:

- Interfere with BECTT operation of computing facilities or e-mail services.
- Interfere with the user's employment or other obligations to BECTT.
- Interfere with the performance of professional duties.
- Is of a reasonable duration and frequency.
- Is performed in non-work time.
- Does not over burden the system or create any additional expense to BECTT.

Such use must not be for:

- Unlawful activities.
- Commercial purposes not under the auspices of BECTT.
- Personal financial gain.
- Personal use inconsistent of BECTT policies or guidelines.

All such use should be done in a manner that does not negatively affect the use of BECTT's systems for business purposes. Employees and trainees are expected to demonstrate a sense of responsibility and not abuse this privilege.

7. Privacy

BECTT respects users' privacy. E-mail content will not be routinely inspected or monitored, nor content disclosed without the originator's consent. However, under the following circumstances such action may be required:

- When required by law.
- If there is a substantiated reason to believe that a breach of the law or BECTT policy has taken place.
- When there are emergency or compelling circumstances.

BECTT reserves the right, at its discretion, to review any employee's or trainee's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other school policies.

Employees should not have any expectation of privacy to his or her Internet usage. BECTT reserves the right to inspect any and all files stored in computers or on the network in order to assure compliance with this policy. Auditors must be given the right of access to any document, information or explanation that they require.

8. Email & internet use at home

Access to the Internet from an employee's or trainee's home using a BECTT owned computer or through BECTT's owned connections must adhere to all the policies that apply to use within BECTT. Family members or other non-employees must not be allowed to access BECTT's computer system or use BECTT's computer facilities, without the formal agreement of the Executive Director.

9. Policy violations

Staff or trainees who abuse the privilege of BECTT facilitated access to electronic media or services face being subjected to disciplinary action, up to and including termination of employment or dismissed from the course immediately and risk having the privilege removed for themselves and possibly other employees or trainees.

Users must not:

- Ignore e-mails. The system is designed for speedy communication.
- If the message requires a reply, a response should be sent promptly.
- Use anonymous mailing services to conceal identity when mailing through the Internet, falsify e-mails to make them appear to originate from someone else, or provide false information to any Internet service which requests name, e-mail address or other details.
- Abuse others (known as 'flaming'), even in response to abuse directed at themselves.
- Use e-mail, either internally or on the Internet, to sexually harass fellow employees, and or trainees, or harass or threaten anyone in any manner.

10. Data protection

The Data Protection Act 1998 prohibits the disclosure of personal data except in accordance with the principles of the Act. This prohibition applies to e-mail in the same way as to other media. Information gathered on the basis that it would be seen by specified employees must not be given to a wider audience. In accordance with the provisions of Article 8 of the European Convention on Human Rights[2], BECTT respects the right to privacy for employees who use IT equipment but does not offer any guarantee of privacy to employees using IT equipment for private purposes.

As data controller, BECTT has responsibility for any data processed or stored on any of its equipment. Any employee monitoring will be carried out in accordance with the principles contained in the Code of Practice issued by the Information Commissioner under the provisions of the Data Protection Act 1998.

In order to comply with its duties under the Human Rights Act 1998, BECTT is required to show that it has acted proportionately, i.e. are not going beyond what is necessary to deal with the abuse and that the need to investigate outweighs the individual's rights to privacy, taking into account BECTTs wider business interests. In drawing up and operating this policy BECTT recognises that the need for any monitoring must be reasonable and proportionate.

Auditors (internal or external) are able to monitor the use of BECTTs IT equipment and the storage of data. They are nevertheless bound by the provisions of the Human Rights Act 1998, the Data

Protection Act 1998, associated codes of practice and other statutory provisions and guidance, including the Regulation of Investigatory Powers Act 2000 in respect of any activity that could be classed as directed surveillance[3]. (See Appendix 2)

---

[2] there shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the county, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[3] Directed surveillance is defined as surveillance which is covert (i.e. carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is our may be taking place) but not intrusive, for the purpose of a specific investigation in such a manner as is likely to result in the obtaining of private information about a person.

11. Email good practice guide

	GOOD PRACTICE
Read Receipt	When it is important to know that a recipient has opened a message, it is recommended that the sender invoke the 'read receipt' option.
Attachment formats	When attaching a file it will have a specific format. Be aware of the possibility that a recipient may not have the software necessary to read the attachment. Format incompatibility can occur even between successive versions of the same software, e.g. different version of Microsoft word.
E-mail Address Groups	If messages are regularly sent to the same group of people, the addressing process can be speeded up by the creation of a personal group in the personal address book.
Message header, or subject	Convey as much information as possible within the size limitation. This will help those who get a lot of e-mails to decide which are most important, or to spot one they are waiting for.
Subject	Avoid sending messages dealing with more than one subject. These are difficult to give a meaningful subject heading to, difficult for the recipient to forward on to others for action, and difficult to achieve.
Recipients	Beware of sending messages to too many recipients at once. When sending messages for more than one-person's use be sure to indicate people for whom there is some expectation of action or who have central interest. Cc to indicate those who have peripheral interest and who are

	not expected to take action or respond unless they wish to do so.
Replying	When replying to a message sent to more than one person, do not routinely reply to all recipients of the original message. Consider who needs to read your reply, e.g. if the sender is organising a meeting and asking you for availability dates, you need only reply to the sender.

	GOOD PRACTICE
Absent	If you have your own e-mail address, it is possible, for users of MS Exchange or have local enhancements to MS-mail, to set the 'out of office' message when you are going to be away for some time, e.g. on annual leave. You won't lose your messages, they will await your return, but the sender will know that you're not there and can take alternative action if necessary.
Evidential Record	Never forget that electronic conversations can produce an evidential record which is absent in a telephone conversation. Comments made by an employee during the course of an exchange of e-mails could be used in support, or in defence, of BECTT's legal position in the event of a dispute.
Legal records	Computer generated information can now be used in evidence in the courts. Conversations conducted over the e-mail can result in legally binding contracts being put into place.
Distribution Lists	Keep personal distribution lists up-to-date and ensure you remove individuals from lists that no longer apply to them.
E-Mail threads	Include the previous message when making a reply. This is called a thread. Threads are a series of responses to an original message. It is best that a response to a message is continued by using reply accessed on the quick menu bar, rather than start an entirely new message for a response. Keep the thread information together. It is easier for the participants to follow the chain of information already exchanged. If the message gets too long the previous parts can be edited while still leaving the essence of the message.

	GOOD PRACTICE
Context	E-mail in the right context, care should be taken to use e-mail where appropriate. There may be occasions when a telephone call would be more appropriate especially on delicate matters. Beware of the use of excessive use of capitals. It can be interpreted as SHOUTING so consider how the style of your email may be interpreted by its recipient.
Forwarding E-mails	Consideration should be given when forwarding e-mails that it may contain information that you should consult with the originator before passing to someone else.

Email good practice guide continued

- **Double check recipients**. Always check that the recipients of e-mail messages are correct before pressing Send to avoid information being sent to the wrong person. This is one of the most common security incidents we come across!
- **Ensure information is available**. Your email system must not be used for filing business information; this information should be in a shared environment where others can refer to it if needed. If an email is about a trainee or a member of staff and it needs to be kept, it should be saved onto the trainee's or staff member's file (either in paper form, or saved directly onto your MIS).
- **Delete if not needed**. If an email does not need to be kept don't bother keeping it! Once you have replied, delete the email.
- **Practice good housekeeping.** Get into the habit of reviewing your emails regularly. It's much easier to delete them little and often, than to be faced with hundreds of emails which can be overwhelming, and you may feel you don't know where to start.
- **Set up delegates**. You should never share your password, but you are able to give delegate rights which will allow other people (we suggest at least 2) to access to your email inbox during any absence. File private emails in a subfolder to ensure they remain private.
- **Manage distribution lists**. If you are the owner of a distribution list or group mailbox, you must ensure you annually review the recipients/members to ensure changes are taken into account.
- **Be wary of Phishing**! If you suspect that there is a virus in an email, you must immediately delete it as a precautionary measure without forwarding the email on to anybody else.
- **Beware auto-forward**. Do not set up an auto-forward rule which re-directs all your emails from your school account to a non-school account. School emails should not be sent to a personal email account.
- **Do not put personal names in the subject line of emails**. If you receive an email containing personal information in the subject line, you must remove it before forwarding/replying
- **Think twice before hitting "reply all"**. Does everyone on the list needs to receive your reply?
- **Add the email address last**. It's so easy to accidentally send an email before you've finished writing it, so only add the email address once you've checked it through and are ready to send.

- **Proofread every message**. Don't just rely on spell-check – if you accidentally write that something contains some "useless information" instead of "useful information", spell-check wouldn't pick that up! Read and re-read before sending your email.
- **Remain professional.** Remember, anyone has the right to request a copy of anything you have recorded about them, and this includes emails. If you have written "if you think Adam is bad, you should meet his mother!" and Mrs Jones subsequently requests a copy of all emails written about herself or her son, that email will have to be released.

12. Legislative framework

The Human Rights Act 1998

This provides for the concept of privacy giving a 'right to respect for private and family life, home and correspondence'. The provision is directly enforceable against public sector employers, and all courts must now interpret existing legislation in relation to the Human Rights Act. Halford v UK 1997 suggests that employees have a reasonable expectation of privacy in the workplace, and employers are recommended to provide workers with some means of making personal communications which are not subject to monitoring, for instance a staff telephone line or a system of sending private e-mails which will not be monitored.

Covert monitoring is likely to be unlawful unless undertaken for specific reasons as set out in the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (see below). Employers should make sure workers know of any monitoring or recording of correspondence (which includes e-mails, use of Internet, telephone calls, faxes and so on).

Regulation of Investigatory Powers Act 2000

This Act covers the extent to which organisations can monitor or record communications at the point at which they enter or are being sent within the employer's or providers telecommunications system and applies to public and private communication networks. If gives the sender or recipient of a communication the right of action for damages against the employer or provider for the unlawful interception of communications.

There are two areas where monitoring is not unlawful. These are:

- Where the employer reasonably believes that the sender and intended recipient have consented to the interception
- Without consent, the employer may monitor in the following circumstances, as set out in the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. these include:

    - To ensure compliance with regulatory practices e.g. Financial Services Authority requirements
    - To ensure standards of service are maintained, e.g. inc all centres
    - To prevent or detect crime
    - To protect the communications system this includes unauthorised use and potential viruses
    - To determine the relevance of the communication to the employer's business i.e. picking up relevant messages when someone is away from work.

However, the employer is expected to make all reasonable efforts to ensure system users know that communications may be intercepted, and any such monitoring must also comply with the provisions of the Data Protection Act 1998 (see below), and in particular the Data Protection principles on fair processing.

EU General Data Protection Regulations (GDPR)

We are committed to protecting the privacy of anyone whose personal data we hold.

As an organisation we have to comply with data protection legislation. From Friday 25 May 2018, the Data Protection Act 1998 will be superseded by the EU General Data Protection Regulations (GDPR) and the UK Data Protection Act 2018 and other supporting data protection legislation (e.g. Privacy Electronic Communications Regulations (PECR)).

Data protection legislation places obligations on us to protect your personal information. We have to make sure we process personal data in line with data protection principles and ensure that your rights as Individuals (Data Subjects) are met.

We have produced a GDPR policy and this will be handed to every trainee at the start of the course, who need to sign confirming it has been read and understood.

Data Protection Act

The Information Commissioner – responsible for enforcement of the Data Protection Act – published four codes of practice to help employers comply with the provisions of the Data Protection Act. These codes clarify the Act in relation to processing of individual data, and the basis for monitoring and retention of email communications.

The code of practice *Monitoring at work: an employer's guide* states that any monitoring of E-mails should only be undertaken where:

- The advantage to the business outweighs the intrusion into the workers' affairs

- Employers carry out an impact assessment of the risk they are trying to avert workers are told they are being monitored
- Information discovered through monitoring is only used for the purpose for which the monitoring was carried out
- The information discovered is kept secure
- Employers are careful when monitoring personal communications such as e-mails which are clearly personal
- Employers only undertake covert monitoring in the rarest circumstances where it is used for the prevention or detection of crime.

Telecommunications (Lawful Business Practise) (Interception of Communications) Regulations 2000

This Act empowered the Secretary of State to make regulations, which allow businesses to intercept communications in the course of lawful business practice and in specific circumstances without the express consent of either the sender or the recipient. Under the Regulations, businesses are required to make all reasonable efforts to inform users of their own systems that such interceptions might take place.

Contract Law

It is just as possible to make a legally binding contract via e-mail as it is by letter or orally. Workers need to be aware of the danger of inadvertently making contracts on behalf of their employer, or varying the terms of any existing contract.

Copyright Law

The Copyright, Designs and Patents Act 1988 (as amended) gives the same protection to digital and electronic publications as it does to printed books and other forms of publication. Many websites carry warnings that the information given is copyright and should not be downloaded without agreement from the copyright holder. Similarly copyright exists over software, which should not be downloaded without license.

Obscene Publications Act 1959, Protection of Children Act 1988, Criminal Justice Act 1988

These Acts are concerned with material that might be criminal, cause harm to young persons or be otherwise unlawful. In the workplace the downloading of certain images from the Internet might subject a worker to charges of criminal behaviour.

Computer Misuse Act 1990

This Act is mainly concerned with the problems of 'hacking' into computer systems.

Lawful Business Practice Regulations (LBP)

The LBP Regulations authorise employers to monitor or record communications without consent for a number of purposes, including the following:

- To establish the existence of facts relevant to the business.

- To ascertain compliance with the regulatory or self regulatory practices or procedures relevant to the business.
- To ascertain or demonstrate standards which are, or ought to be, achieved by persons using the system
- To prevent or detect crime.
- To investigate or detect the unauthorised use of telecommunication systems.

The Regulations cover all types of communications including those that are Internet based, by fax and by email.

July 2021