Bespoke Training & Education
INTERNET, EMAIL AND SOCIAL MEDIA POLICY – Review Feb 2027

1. AIMS AND OBJECTIVES

1.1 |Bespoke Training & Education (BT&E) recognises that the internet and email systems play a key role in the conduct of the business and that these systems support employees in carrying out their work efficiently. It also recognises the value that social media can have to our business if used in a responsible and professional way. Nevertheless, the provision of internet and email systems to employees, as well as access to social media both in and outside the workplace, does expose BT&E to a number of risks and liabilities.

This Policy highlights those potential liabilities to ensure that employees understand how they should be avoided and are informed of the expectations for the use of those resources, incorporating authorised access to social media, to ensure that they are used appropriately.

1.2 While it is recognised that employees are entitled to a private life, we are committed to maintaining confidentiality and professionalism at all times whilst also upholding its reputation by ensuring employees exhibit acceptable behaviours. To this end, the policy outlines the responsibilities of employees when accessing social media personally to ensure that its use in this context also avoids bringing BT&E into disrepute. It also supports the aims of BT&E's Code of Conduct for Staff.

1.3 For the clarification in the context of this policy, social media is the term used to describe the online tools, websites and interactive media that enable users to interact with each other in various ways, through sharing information, opinions, knowledge and interests. Social media involves building online communities or networks, which encourage participation, dialogue and involvement.

2. SCOPE

This policy applies to all employees employed by BT&E. Our commitment to equality of opportunity also extends to applicants who apply to work in BT&E establishments. Although this policy refers to employees throughout, we are aware of its wider responsibilities to provide a positive working environment for all who work for us.

Individuals are personally accountable for their behaviour and may be held liable for any breaches of this policy. All individuals who work on BT&E premises, including agency, contract workers and volunteers are therefore expected to support the policy on Internet, Email and Social Media Policy.

3. LEGISLATION

BT&E will adhere to its obligations under the legislation relevant to the use and monitoring of electronic communications, which are predominantly the Regulation of Investigatory Powers Act 2000; the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000; the Communications Act 2003; Data Protection Act 1998; the Human Rights Act 1998; the Defamation Act 1996 and the Equality Act 2010.

4. DATA PROTECTION AND MONITORING

4.1 Computers are the property of BT&E and are primarily designed to assist in the performance of work duties. To ensure appropriate use of the internet, BT&E's internet software monitors all websites visited by employees for business and security purposes. Therefore, employees should have no expectation of privacy when it comes to the sites they access from computers and devices.

4.2 BT&E monitors internet access and emails for business and security purposes and to ensure that employees make appropriate use of the systems at all times.

4.3 BT&E may exercise its rights to intercept internet access under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 for the following business reasons:

- To establish the existence of facts relevant to the business.
- To ascertain compliance with regulatory practices or procedures relevant to the BT&E
- To ensure that employees using the system are achieving the standards required.
- To prevent or detect crime.
- To investigate or detect the unauthorised use or abuse of the telecommunications systems, including using social media websites.
- To ensure effective operation of systems, e.g. to detect computer viruses and to maintain an adequate level of security.

4.4 To be able to exercise its rights, BT&E must make all reasonable efforts to inform every person who may use the internet systems that monitoring may take place. The communication of this policy to all employees meets this requirement and employees are required to sign to confirm that they have read and understood this policy.

5. GENERAL OPERATING PRINCIPLES AND PERSONAL USAGE

5.1 The email and internet systems are primarily for business use.

5.2 BT&E operates within a framework of mutual trust and recognises that in certain circumstances, particularly when there is a need to communicate urgently, it may be appropriate for employees to send and receive personal emails. However, such reasonable private usage of email must not interfere with employees' work. Excessive private use of the email system during working hours will lead to disciplinary action and may in certain circumstances be treated as gross misconduct.

5.3 BT&E also recognises that there may be need for individuals to have to carry out personal tasks on the internet whilst at work. However, where such a need arises, employees are required to limit their access to the internet for personal usage to authorised breaks, lunch breaks or just before or just after their normal working hours. Personal use of the internet during working hours may lead to disciplinary action and excessive personal use may in certain circumstances be treated as gross misconduct.

5.4 Personal use of social media sites through BT&E network is not permitted. Whilst most staff do not have access to social media sites via the college network, on occasion access ma y be granted to undertake a project or particular activity linked to their role.

5.5 Personal usage of the email and internet facilities must still adhere to the standards outlined in this Policy and in other BT&E policies, such as the Bullying and Harassment Policy. Breaches of policies through personal use of email and internet will be dealt with under the BTT&E Disciplinary procedures.

5.6 The standards set out in this Policy are designed to minimise the risk of incurring liability in relation to employees' usage of email and internet. We will take disciplinary action against any employee who breaches any of the requirements contained in this Policy, which will include summary dismissal for those committing acts of gross misconduct.

5.7 BT&E Grievance Procedure will be used to handle any disputes concerning the operation or application of this Policy.

5.8 Each employee is issued with a unique password for use of BT&E computer systems, for security purposes. Employees are responsible for safeguarding their password. For reasons of security, employees must not print, store online or share their individual passwords with others. User password rights are given to employees for security purposes and should therefore not give rise to an expectation of privacy.

6. EMAILS

6.1 General

Although an email that is clearly marked as private cannot be defined as a communication relevant to the business, BT&E reserves the right to monitor the content of such an email where there is a reasonable belief that it may breach this Policy, for example by containing discriminatory or pornographic material.

For business continuity purposes, BT&E may need to check the emails of employees who are absent. BT&E will gain the permission of the employee concerned before undertaking monitoring emails in such circumstances.

All employees are also required to include a disclaimer at the end of all emails, which will advise external recipients and senders of email of the Policy (refer to clause 10, below).

BT&E reserves the right to use the content of any employee email in any disciplinary process.

Employees should note that all emails can be recovered even after they have been deleted.

BT&E reserves the right to inspect any files stored by employees in private areas of the computer system in order to assure compliance with this Policy.

6.2 Standard email practice

- Emails should be drafted with care. Due to the informal nature of email, it can be easy to forget that it is a permanent form of written communication and that material can be recovered even when it has been deleted.

- Employees should ensure that the content and tone of emails reflect the professional image of BT&E.

- All emails should be composed according to BT&E style guidelines: available from Graham Coffey.

- Emails should be clear and concise and should not be any longer than necessary.

- Employees should not send unnecessary emails, or copy other recipients into messages without good reason. Unnecessary emails waste recipients' time and congest the email system.

- Employees should not attach unnecessary files as large attachments can congest recipients' systems.

- Emails should not be written in capital letters as this can be construed as shouting via email.

- Hard copies should always be made of emails which need to be retained for record-keeping purposes.

6.3 Use of email

6.3.1 Employees must never access another employee's email account; except in circumstances where an employee is absent from work and has given his or her express consent for a colleague to check his or her emails. Even where access is granted in such circumstances, employees must never send an email from that account; instead response emails should be sent from the individual's own BT&E email account, clearly marked as being "on behalf of" the original recipient.

6.3.2 Emails must not contain any message or image that is discriminatory (on the grounds of sex, race, disability, sexual orientation, religion, belief or age), illegal, obscene, pornographic, abusive or threatening. BT&E does not tolerate discrimination, harassment or bullying and any breach of this rule will constitute gross misconduct.

6.3.3 Employees should not make derogatory remarks in emails about colleagues, students, competitors, employers or any other person. Written derogatory remarks could be considered to be defamation, which could give rise to legal action being taken against the author and/or BT&E.

6.3.4 Employees may have to send confidential information by email as part of their duties. Employees must exercise caution when sending confidential information, ensuring that it is being sent for a legitimate reason and checking the accuracy of the name and email address of recipients. These emails should be also be flagged as confidential.

6.3.5 Employees must not enter into contractual commitments by email. It is easy for email to be viewed as an informal means of communication, but commitments entered into in emails will have the same weight and status as any other written contracts.

6.3.6 Employees must not begin or distribute chain emails or another other junk emails, including jokes.

6.3.7 Employees must not send personal data of other employees, students, or clients via email, without the authorisation of the owners of that data.

6.3.8 By sending emails on the system, employees are consenting to the processing of any of their personal data contained in that email and are explicitly consenting to the processing of any of their sensitive personal data contained in that email. If employees do not wish BT&E to process such data, they should communicate that information by other means.

7. INTERNET

7.1 Use of internet

7.1.1. BT&E has software and systems in place that monitor and record all internet usage. Therefore, employees should not have any expectation of privacy in terms of their internet usage.

7.1.2 Employees must not display, download, distribute, store, edit or record any material, including images, that are offensive, capable of constituting any form of discrimination (on the grounds of sex, race, disability, sexual orientation, religion, belief or age), obscene, pornographic or paedophiliac. Any such action will be considered as gross misconduct.

7.1.3 Employees must not display, distribute, store or download any illegal material. Any such action will be considered as gross misconduct.

7.1.4 The internet facilities must not be used to undertake illegal activity. Any such action will be considered as gross misconduct.

7.1.5 Employees must not download or distribute any pirated software using the internet system. Any such action will be considered as gross misconduct.

7.1.6 BT&E will retain the copyright to any material posted on the internet by any employee during the course of his or her duties.

7.1.7 Employees must not use the internet facilities to download entertainment software, including games, and must not play games against other opponents over the internet.

7.1.8 Any attempts to disable, defeat or circumvent any of the computer security facilities will constitute gross misconduct.

7.1.9 Whilst BT&E recognises employees' right to a private life, during any use of social networking sites or maintenance of personal blogs (online diaries), employees are required to refrain from making any references to BT&E that could bring it into disrepute, or interacting or writing on the sites in a way that could constitute harassment of a colleague, student or employer. BT&E will treat any breaches of these requirements as disciplinary offences. As with any other personal usage of the internet, employees are not permitted to write on personal blogs or access social networking sites during working hours.

7.1.10 BT&E reserves the right to withdraw at any time employees' access to social networking sites or personal blogs.

7.1.11 BT&E employees must never engage in political discussions through outside newsgroups using the computer system.

7.2. Copyright and downloading

7.2.1 Copyright applies to all text, pictures, video and sound, including those sent by email or on the Internet. Files containing such copyright protected material may be downloaded, but not forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate.

7.2.2 Employees are not permitted to download screensavers for use on the computers.

7.2.3 Employees are not permitted to use the internet facilities to download entertainment images or videos for personal usage.

7.2.4 Any file that is downloaded must be scanned for viruses before it is run or accessed.

8. SOCIAL MEDIA

8.1 General

Access to social media sites is restricted on the network to employees using it as part of their role. However, the expectations for staff to behave appropriately to avoid risks and liability to BT&E extends to personal use outside of work.

8.2 Privacy settings and personal information

Default privacy settings for some social media websites allow some information to be shared beyond an individual's contacts. In such situations, the user of the site is personally responsible for adjusting the privacy settings for the account. Information available on social media sites could be produced as evidence by either BT&E or employee, should it be necessary either as part of BT&E procedures, or in legal proceedings.

Therefore, it is vital that employees and students are strongly encouraged to review their access and privacy settings for any social media sites to control, restrict and guard against who can access the information on those sites. Even if privacy and security settings are utilised, anything posted on social media sites may be made public by onward transmission.
Social media offers the ability to share personal information rapidly and easily. Employees should have particular regard to protecting passwords and personal information to reduce the risks of abuses such as identity theft.

To avoid identity theft, employees are advised to refrain from publishing any personal or sensitive information on social media websites, e.g. date of birth, home address, telephone number or any information related to personal bank accounts.

8.3 Acceptable use of social media at work

The IT Systems are first and foremost business tools, and as such personal usage of the systems is a privilege and not a right. Employees are permitted to make reasonable and appropriate use of social media websites where this is part of the normal duties of their work.

Employees responsible for contributing to the BT&E social media activities should be aware at all times that they are representing BT&E. Employees who use social media as part of their job should adhere to the rules and standards set out in paragraph 6.2.

Employees must not use BT&E IT networks to use social media channels other than if it a part of their job role at BT&E. It is not permitted to use its IT networks to communicate personally with friends; indeed, normally access to these sites is revoked other than for those using it as part of their job.

Employees may wish to use their own personal devices (including laptops, palm-tops, hand-held devices and smart phones) to access social media websites while at work. Employees should limit their use of social media on their own personal equipment to their official rest breaks and/or when between appointments when travelling and/or times when they are not on duty e.g. before and after work.

Personal use of social media should not interfere with employees' work duties and responsibilities. Excessive personal use of social media website and abuse of this policy will be considered a disciplinary offence.

8.4 Expected standards of conduct on social media websites

8.4.1 Appropriate conduct

The line between public and private, professional and personal is not always clearly defined when using social media. If an employee identifies themselves as a member of staff, the potential to create perceptions about BT&E to a range of external audiences and also among colleagues and students.

When communicating either in a professional or personal capacity, within or outside the workplace, employees must:

- Conduct themselves in accordance with other policies, procedures and the Code of Conduct for Staff particularly when using BT&E social media accounts to portray the BT&E activities, as this is an extension of BT&E infrastructure.

- Be professional, courteous and respectful as would be expected in any other situation.

- Think carefully about how and what activities are carried out on social media websites.

- Be transparent and honest. BT&E will not tolerate employees making false representations. If employees express personal views, it should be made clear that the views do not represent or reflect the views of BT&E.

- Remove or request the removal of any inappropriate comments, images or videos of them.

8.4.2 Inappropriate conduct

While using social media in any capacity, employees' actions can still damage BT&E reputation.

When communicating either in a professional or personal capacity, within or outside the workplace, employees must conduct themselves appropriately. The following are examples of inappropriate conduct:

- Engaging in activities that have the potential to bring BT&E into disrepute.
- Breach of confidentiality by disclosing privileged, sensitive and/or confidential information.
- Making comments that could be considered to be bullying, harassing or discriminatory against any individual.
- Posting remarks which may inadvertently cause offence and constitute unlawful discrimination, harassment and/or victimisation.
- Posting or uploading inappropriate comments, images, photographs and/or video clips about colleagues or ex-colleagues, students or ex-students, parents or clients.
- Publishing defamatory and/or knowingly false material about BT&E, other employees or students.
- Engaging in discussions or anything which may contravene the equality and diversity policy and may have the potential to cause serious harm to the business.
- Use of offensive, derogatory or intimidating language which may damage working relationships.
- Blurring the boundaries of professional and personal life.
- Pursuing personal relationships with students, ex-students or parents.
- Participating in any activity which may compromise your position at BT&E.
- Behaviour that would not be acceptable in any other situation.
- Knowingly accessing, viewing or downloading material which could cause offence to other people or may be illegal.
- Commenting on any work-related matters.
- Posting any material that breaches copyright legislation.

- Using a BT&E email account to create a personal social media account.
- Doing anything that may conflict with the interests of BT&E
- Using social media websites in any way which is deemed to be unlawful.

The above examples are not exhaustive or exclusive.

Employees will be held personally liable for any material published on social media websites that compromise themselves, their colleagues and/or BT&E.

8.4.3 Acceptance of friends

Social media is used by many people, particularly students to communicate with their peers and the public.

Students may wish to form personal relationships with employees, however to ensure professional boundaries are maintained, employees must not accept and/or invite the following individuals to be 'friends' on personal social media accounts or other online services:

- Students, including vulnerable students who are adults or children,
- Ex-students under the age of 18, and
- Parents (except where the friendship pre-exists and/or is as a result of a situation not related to their child being a student at the college).

Entering into such relationships may lead to abuse of an employee's position of trust and breach the standards of professional behaviour and conduct expected at BT&E. We reserve the right to take disciplinary action if employees are found to be in breach of this policy, with the potential of dismissal for serious breaches.

Acts of a criminal nature or any safeguarding concerns may be referred to the police, Local Safeguarding Children Board (LSCB) and/or the Independent Safeguarding Authority (ISA).

8.5 Use of social media during recruitment and selection process

BT&E will only view relevant social media websites as part of the pre-employment process, i.e. those aimed specifically at the professional market and used for networking and career development (e.g. LinkedIn). Any information that relates to applicants' protected characteristics under the Equality Act 2010 will not be used as part of the recruitment and selection process.

\8.6 Inappropriate conduct and excessive use

Any breach of this policy, including inappropriate conduct of the kind listed in section 7 above, or of a similar nature, and any excessive personal use of social media websites will be dealt with in accordance with BT&E disciplinary procedure.

Disciplinary action may be taken against employees in line with BT&E disciplinary policy and may also result in withdrawal of internet access. Persistent breaches of this policy may lead to dismissal. Serious cases may be treated as gross misconduct, which may result in summary dismissal.

9. RESPONSIBILITIES

The responsibility for drafting, updating, monitoring and reviewing this policy belongs to Graham Coffey. It will be reviewed on a yearly basis.

All employees are responsible for complying with the requirements of this policy and for reporting any breaches of the policy to Graham Coffey.

If employees have concerns about information or conduct on social media sites that are inappropriate, offensive, demeaning or could be seen to be bullying, this should be reported to their line manager and Graham Coffey.

10. INFORMED CONSENT

All employees are required to sign to confirm that they have read and understood this policy and agree to comply with its requirements. This will be recorded via the induction programme signing sheet, which is kept as a record of your CPD.