Bespoke Training & Education (BT&E) – Review: Sept 25

E-Safety and Acceptable Use of Internet Policy

The e-Safety Policy relates to other policies including those for Computing, Anti- Bullying and for Safeguarding and Child Protection. BT&E director will oversee this area.

Our E-Safety Policy has been written by Bright HR.

Teaching and learning • The Internet is an essential element in 21st century life for education, business and social interaction. BT&E has a duty to provide students with quality Internet access as part of their learning experience. • Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. • Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. • Students will be taught what Internet use is acceptable and what is not. They will be given clear objectives for Internet use. • Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation • Students will be taught how to evaluate Internet content • Students will be taught the importance of cross-checking information before accepting its accuracy. • Students will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protector.

Information system security • Computing systems security will be reviewed regularly. • Virus protection will be updated regularly. • Security strategies will be discussed with our consultants. Published content and the BT&E web site • Staff or students personal contact information will not generally be published. The contact details given online should be BT&E head office. • BT&E director will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing students images and work • Photographs that include students will be selected carefully to minimize the risk that their image is misused. Staff will consider using group photographs rather than full-face photos of individuals. • Full names will not be used anywhere on a BT&E website or other non-secure on-line space, particularly in association with photographs. • Written permission from parents or carers will be obtained before photographs of students are published on the Website. • Image file names will not refer to the student by name. • Parents should be clearly informed of the policy on image taking and publishing.

Cyberbullying: Is bullying through the use of communication technology and can take many forms e.g. sending threatening or abusive text messages or e-mails either personally or anonymously, making insulting comments about someone on a social networking site or blog or making/sharing derogatory or embarrassing videos of someone via mobile phone or e-mail. BT&E will explain that this behaviour is inappropriate and that, where appropriate, relevant people and professionals will be contacted (which may include the police and parents).

Social networking and personal publishing • BT&E will control access to social networking sites, and consider how to educate students in their safe use. • Studentls will be taught that social network sites have age restrictions, and Primary aged children should not have a profile on any social networking site. • Students will be taught and advised never to give out personal details of any kind which may identify them, their friends or their location. • Students and parents will be advised that the use of social network spaces outside can bring a range of dangers for students. • Students will be advised to use nicknames and avatars when online. • Students who have permission to use their mobile phones are required to follow the policy for mobile phones with regard to social networking.

E-mail • Students may only use approved e-mail accounts on the school system. • They must immediately tell a teacher if they receive offensive e-mail. • In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission from an adult. • Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known. • BT&E will consider how e-mail from students to external bodies is presented and controlled. • The forwarding of chain letters is not permitted.

Authorising Internet access • All staff must read and sign the “Acceptable Use Policy” before using any IT resource. • At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials. • Any person not directly employed by the school will be asked to sign an “acceptable use of BT&E IT resources” before being allowed to access the internet from the site.

Assessing risks • We will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither BT&E or its IT consultants can accept liability for any material accessed, or any consequences of Internet access. • BT&E will audit IT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints • Complaints of Internet misuse will be dealt with by a senior member of staff. • Any complaint about staff misuse must be referred to BT&E director. • Complaints of a child protection nature must be dealt with in accordance with BT&E's safeguarding procedures. • Students and parents will be informed of the complaints procedure (see BT&E complaints policy) • Students and parents will be informed of consequences for pupils misusing the Internet.

Communications Policy Introducing the e-safety policy to pupils • E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly. • Students will be informed that network and Internet use will be monitored and appropriately followed up. • E-Safety training will be embedded within the IT scheme of work or the Personal Social and Health Education (PSHCE) curriculum.

Staff and the e-Safety policy • All staff will be given the BT&E e-Safety Policy and its importance explained. • Staff must be informed that network and Internet traffic can be monitored and traced to the individual user. • Staff who manage filtering systems or monitor IT use will be supervised by senior management and work to clear procedures for reporting issues. • Staff will promote the use of a student friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support • Parents' and carers' attention will be drawn to BT&E e-Safety Policy in newsletters, the brochure and on the web site and be required to adhere to the Home School Agreement. • BT&E will maintain a list of e-safety resources for parents/carers. • BT&E will ask all new parents to sign the parent /pupil agreement when they register their child with BT&E. • Parents will be invited to learn about e-safety through parents information sessions which will be held at regular intervals and appropriate e-safety information will be sent home when available. Guidance on how to deal with Cyberbullying and Internet Safety can be found in the main Safeguarding file held in the director's office.

General: Students are responsible for good behaviour on the Internet, just as they are in the classroom or any other provision they are attending with BT&E.

General rules apply. The Internet is provided for students to conduct research and communicate with others. Parents' permission is required. Remember that access is a privilege, not a right and that access requires responsibility. Individual users of the Internet are responsible for their behaviour and communications over the network. It is presumed that users will comply with BT&E standards and will honour the agreements they have signed. Computer storage areas and memory sticks will be treated like lockers.

Staff may review files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on servers or sticks will always be private. All memory sticks and cds brought from home should be scanned for viruses before use.

Teachers will guide students towards appropriate materials. Outside BT&E, families will bear responsibility for such guidance, as they must also exercise with information sources such as television, films, radio and other potentially offensive media.

The following are not permitted:

1. Sending or displaying offensive pictures or messages or pictures.

2. Using obscene language.

3. Harassing, insulting or attacking others.

4. Damaging computers, computer systems or computer networks.

5. Violating copyright laws.

6. Using others' passwords.

7. Trespassing in others' work folders, work or files.

8. Intentionally wasting limited resources.

Sanctions

1. Violations of the above rules will result in a temporary or permanent ban on Internet use.

2. Additional disciplinary action may be added in line with BT&E's Behaviour Policy on inappropriate language or behaviour.

3. When applicable, the police or local authorities may be involved.

Adapted from National Association for Co-ordinators and Teachers of Computing.

E-Safety Rules

▪ Ask permission before using the internet

▪ Tell a trusted adult if you see anything that makes you feel uncomfortable

▪ Immediately close any webpage that you are uncomfortable with

▪ Do not give out any personal information such as name, address, telephone number(s), age, school name or bank card details

▪ Make sure that when using social networking sites, privacy settings are checked so that not just anyone can see your page/photos

▪ Only contact people that you have actually met in the real world

▪ Never arrange to meet someone that you have only met on the internet

▪ Only use a webcam with people you know – Always ask an adult before using the camera function on a device

▪ Think very carefully about any pictures that you post online

▪ Never be mean or nasty to anyone on the internet or when using a mobile phone. If you know of someone being mean to another person, tell a trusted adult

▪ Only open e-mails from people that you know

▪ Avoid using websites that you wouldn't tell anyone about and use a student friendly search engine such as http://www.askforkids.com

MANAGING INCIDENTS

The organisation manager/e-safety lead/child protection lead will ensure that an adult follows these procedures in the event of any misuse of the internet:

Has there been inappropriate contact?

1. Report to the designated Safeguarding Lead (or the Deputy)

2. Advise the child, young person or vulnerable adult on how to terminate the communication and save all evidence

3. Contact the parent(s)/carer(s)

4. Contact the police on 101

5. Log the incident

6. Identify support for the child, young person or vulnerable adult.

Has someone been bullied?

1. Report to the designated Safeguarding Lead (or the Deputy)

2. Advise the child, young person or vulnerable adult not to respond to the message

3. Refer to relevant policies including anti-bullying, e-safety and AUP and apply appropriate sanctions

4. Secure and preserve any evidence

5. Contact the parent(s)/carer(s)

6. Consider informing the police on 101, depending on the severity or repetitious nature of the offence

7. Log the incident

8. Identify support for the child, young person or vulnerable adult.

Has someone made malicious/threatening comments? (child/young person/vulnerable adult or organisation staff/volunteer)

1. Report to the DSL or Deputy

2. Secure and preserve any evidence

3. In the case of offending web-based e-mails being received, capture/copy the 'header' info, if possible.

4. Inform and request that the comments are removed from the site/block the sender

5. Inform the police on 101 as appropriate

6. Log the incident

7. Identify support for the child, young person or vulnerable adult.

Has an inappropriate/illegal website been viewed?

1. Report to the DSL or Deputy

2. If illegal do not log off the computer but disconnect from the electricity supply to the monitor and contact the police on 101

3. Record the website address as well as the date and time of access

4. If inappropriate refer the child/young person/vulnerable adult to the AUP that was agreed and reinforce the message

5. Decide on the appropriate sanction

6. Inform the parent(s)/carer(s)

7. Contact the filtering software provider to notify them of the website.

TRAINING &
BESPOKE
EDUCATION

ACCEPTABLE USE POLICY (AUP) FOR STAFF AND VOLUNTEERS

Please sign and return to BT&E Office.

This covers use of digital technologies in the organisation i.e. e-mail, internet, and network resources, learning platforms, software, mobile technologies, equipment and systems.

Any questions you may have regarding e-safety or the acceptable use of the IT facilities should be directed to Graham Coffey - Designated Safeguarding Lead)

By signing this form, you agree to the following conditions:

• I will only use the organisation's digital technology resources and systems for professional purposes or for uses deemed reasonable by the manager.

• I will only use an e-mail account allocated by BT&E.

• I will not browse, download or send material that could be considered offensive to colleagues and any other individuals.

• I will report any accidental access, receipt of inappropriate materials or filtering breaches to the manager

• I will not allow unauthorised individuals to access e-mail / internet / networks of systems.

• I will ensure that all my login credentials (including passwords) are only shared with the IT Technician and BT&E director.

• I will not download any software or resources from the internet that can compromise the network or are not adequately licensed. I will speak to the IT Technician if I find software on the Internet I wish to have on my laptop.

• I will follow the DSCF 2009 'Guidance for Safer Working Practice for Adults who work with Children and Young People'

• I will ensure that my personal e-mail accounts, mobile/home telephone numbers are not shared with children, young people or families.

• I will not allow children and young people to add me as a friend to their social networking site nor will I add them as friends to my social networking site.

• I will ensure that any private social networking sites / blogs, including Facebook and Twitter, etc. that I create or actively contribute to are not confused with my professional role.

- I understand that all internet and network usage can be logged and this information could be made available to my manager on request.

- I will not connect a computer, laptop or other device to the network/internet that has not been approved by the organisation and meets its minimum security specification. If using my own USB I will ensure it is always scanned for viruses.

- I will not allow students to use a laptop / whiteboard that have been assigned to me. I understand that I will not loan my laptop to family members or friends.

- I will bring my laptop to work on a daily basis.

- If I no longer work at the school I will return my laptop to the School Bursar with all other electronic devices.

- Visitors to the school who require access to the internet can only do so with the permission of those named above.

- I will not use the camera facility on a mobile phone to take pictures of students of young people.

- I will not use the IT facilities for personal reasons at any time when I am not on a timetabled break, including during directed time after lessons.

- I will not use personal digital cameras or camera phones for transferring images of children and young people or staff without written permission.

- I will not engage in any online activity that may compromise my professional responsibilities.

- I understand that the Data Protection Act requires that any information seen by me with regard to staff or children and young people, held within any organisation system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

- I will at all times behave responsibly and professionally in the digital world and will not publish any work-related content on the internet.

- I will ensure that I am aware of digital safeguarding issues so that they are appropriately embedded in my practice.

- I understand that failure to comply with the Acceptable Use Policy (AUP) could lead to disciplinary action. Social Networking Sites

- At home, I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role. I will not use these forums to make any comments in relation to the school, colleagues or students or to post any information relating to the school including photographs. Ratified by Governing Body: February 2022 12 Review Date: February 2024

- I will not access social networking sites such as Facebook or MySpace while using the IT facilities or on my BT&E laptop in or out of lessons and preparation time.

- I will not accept 'Friend Requests' from the parents of pupils.

- I will not share information about BT&E in internet forums as it is unacceptable and can bring the company and / or the clients BT&E works with into disrepute and put young people at risk.

If I see or become aware of inappropriate information about staff or children through conversations with colleagues, parents or partners, I understand that I have a responsibility to alert BT&E.

I will keep this information confidential in line with the Data Protection Act and within BT&E's safeguarding policy.

However, there may be times when I am required to disclose information to an appropriate authority such as the Police or Children's Social Care. In such cases, I can see advice from BT&E safeguarding officer or Local Authority HR.

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand BT&E's most recent Acceptable Use Policy (AUP). I agree to abide by the most recent Acceptable Use Policy (AUP).

Signature …………………………………………….. Date ……………………………

Full Name ……………………………………………………………………………………. (print)

Job title …………………………………………………………………………………………….

Organisation BESPOKE TRAINING AND EDUCATION Ltd

BT&E **Authorised Signature/Manager**

I approve this user to be set up Signature …………………………………………….. Date …………………………….
Full Name……………………………………………….

Job Title ……………………………….