BOHUNT EDUCATION TRUST EMAIL, INTERNET AND

COMMUNICATIONS POLICY

Contents

1. POLICY STATEMENT

1.1 This policy aims to outline the duties and procedures adopted by the employer (referred to as Bohunt Education Trust, the Trust or BET) for the use of its information communication technology (ICT) facilities, and to set out professional boundaries regarding communication between employees and students.

1.2 This policy applies to all employees of BET schools who make up the Trust.

1.3 The Trust encourages its employees to use its ICT facilities wherever appropriate and particularly when this saves time and expense and increases efficiency.

1.4 Inappropriate use can cause many problems ranging from minor distractions to legal claims against BET. Any employee who is unsure about whether or not their actions may constitute a breach of this policy should seek advice from their manager or Headteacher.

1.5 This policy is designed to protect all persons referred to above from the consequences of misuse of ICT and to provide guidelines to users about appropriate use of the Trust's ICT facilities.

1.6 BET is committed to safeguarding children and protecting both its interests and those of its employees through the use of all (ICT) facilities.

1.7 This policy applies to all users of the Trust's ICT facilities, including but not limited to all employees, students, governors, directors, contractors, agency workers, associates and visitors.

1.8 Those who work for the Trust are not permitted to connect personal devices (e.g. smart phones, tablets, laptops, etc.) to BET's systems without the express prior consent of the Headteacher.

1.9 Where personal devices are brought to work for personal use they must only be used privately.

1.10 Those who connect personal devices to the Trust's systems must also comply with this policy.

1.11 Employees must take care not to introduce viruses on to the system and must take proper account of the security advice below.

1.12 Employees must also ensure that they do not send libellous statements in electronic communications (or at all).

1.13 This policy is not contractual and can be replaced or amended by the Trust from time to time as may be required.

2. DEFINITIONS

2.1 In this policy the following meanings shall apply:

- ICT means any of the ICT facilities used on the Trust's premises, including email, the internet and other networks, all computers, webcams, data storage devices, mobile telephones, cameras, tablets (e.g. iPads or similar) and any related software and/or hardware.

- Information means information in any format belonging to the Trust or otherwise used in your job or studies whether or not marked as private or confidential.

- Correspondence includes any communication as part of your job or studies in any format e.g. personal conversation, telephone voicemail, email, text messages or graphics.

- PC means any laptop or computer or any smart phone or tablets or electronic devices that have the capability to carry out functions the same or similar to those functions that are carried out on a computer.

- User means any person to whom this policy applies and who uses ICT as defined above.

3. SECURITY

3.1 Users must not carry out any action that interferes with the normal working of the ICT. This prohibition includes but is not limited to:

- Downloading any computer programme, software or executable file;
- Downloading any ordinary file (e.g. pdf or Microsoft Office document) from a source that is not totally reputable and trustworthy;
- Saving any file that is received electronically from an unknown third party onto the ICT;
- Accessing any data on the ICT without the Headteacher's express consent
- Modifying or otherwise risking the corruption of any data on the ICT

3.2 Users must be mindful at all times that files, programmes, software etc. may contain embedded viruses or other malicious code that could damage ICT.

3.3. If there is a need for additional software to be installed onto a PC then the user should submit a request to their manager and/or the Headteacher.

3.4 Any user who deliberately introduces any virus or other malicious code will be dealt with under the Disciplinary Policy.

3.5 If a virus or other alert comes to the attention of a user then that person must stop what they are doing immediately and report it to someone in the IT department.

3.6 Users must ensure that ICT is left 'safe' when they are not using it (i.e. that is cannot be accessed by someone else). For example, a PC must be 'screen locked' when a user leaves their desk. Users may be held responsible for any inappropriate use of, or access to, ICT using their log on details.

3.7 Users must not allow students to use or access ICT that is not specifically designated for their use.

3.8 For further email and social media information, see Social Media policy for Bohunt Education Trust.

3.9 Users may only use ICT for commercial activities if they are an employee of BET and only when such use forms part of their work duties. If there is any doubt about a particular activity guidance should be sought from the user's manager or the Headteacher.

3.10 Non-educational games must not be installed or played on the ICT.

3.11 Users must not tamper with the configuration of any PC or any cables or peripheral devices attached to PCs.

3.12 Users must take care not to damage any of the ICT (e.g. users must not store or consume food or drink close to a PC, must follow all user manuals and instructions, etc.)

3.13 ICT that is portable must be kept in a secure place when not in use and stored in a case, bag or container to protect it from damage.

3.14 When being transported portable ICT should be kept in a vehicle's boot or other lockable storage area.

3.15 Loss, damage or theft of ICT as a result of misuse, or negligence may where appropriate result in a final sanction for any user who is responsible for the same.

3.16 The Trust may monitor its systems and related ICT usage.

4. PASSWORDS

41. Users who are permitted to access or use the ICT in question will be issued with logon and password details for all ICT that is capable of being password protected.

4.2 Users must keep details of their usernames and passwords confidential.

4.3 Passwords should be changed at regular intervals and include a mix of upper and lower case letters, numbers and other characters. Obvious passwords (for example those that include the user's date of birth or name) should not be used.

4.4 Passwords should not be written down unless absolutely necessary and if they are noted in writing they should be kept separately with some obvious characters omitted. These may not be disclosed to other users or individuals.

4.5 Logon IDs and password may not be shared between users. Access to ICT using another user's log on details may result in disciplinary action.

4.6 All sensitive documents should be password protected.

5. USE OF EMAIL

5.1 The Trust's email system is available for communication on matters directly concerned with the Trust and a user's duties and responsibilities in relation to the Trust; it should only be used for these purposes. Users must pay particular attention to the following points.

5.2 Records

5.2.1 Users must ensure that copies of all incoming and outgoing emails, including attachments, are kept.

5.3 The extent of circulation

5.3.1 Users must ensure that emails are sent only to the intended and relevant recipients. This applies particularly when forwarding or replying to external emails where misdistribution of sensitive information could have legal implications.

5.3.2 Internal email messages should only be sent to those for whom they are relevant.

5.3.3 users should not copy emails automatically to all those copied into the original message to which they are replying. Doing so may result in disclosure of confidential information to inappropriate recipients. Users must ensure all recipients are appropriate given the content of the message and the identity of other recipients.

5.4 Content

5.4.1 Internal emails may be sent in an informal style; however users must observe the normal courtesies of correspondence.

5.4.2 Emails and any email attachments should be checked carefully to ensure the contents are correct, as once sent they cannot be retrieved. It is good practice to re-read emails before sending.

5.4.3 Emails are like any form of written communication and, as such, what is normally regarded as unacceptable will also be unacceptable in an email communication.

5.5. The appropriateness of email

5.5.1 Emails should seldom be used as a substitute for face-to-face communication. It may be appropriate or helpful to send a brief note by email confirming a discussion, however, it is likely to appear hostile and unfriendly if users rely entirely upon email to communicate with one another.

5.5.2 'Flame' emails (emails that are abusive) are likely to be a source of stress and damage work relationships, and can be regarded as cyber bullying. Hasty messages, sent without proper consideration, can cause unnecessary misunderstandings and should be avoided.

5.5.3 The use of capital letters in emails may be regarded as 'shouting' at the recipients and must be avoided.

5.5.4 The use of swear words or obscene language is prohibited. Users musts ensure that emails, including forwarded or attached content, will not cause offence to any recipient/s (either an intended, or possible end recipient).

5.5.5 Users must not use email to send or forward messages that are defamatory, obscene or otherwise inappropriate. In serious cases this could be regarded as Gross Misconduct and could lead to dismissal. If a user receives an obscene or defamatory email, whether unwittingly or otherwise and from whatever source, they should not forward it to any other address and should notify the Headteacher.

5.5.6 Statements of adverse opinion other than properly expressed in the context of established Trust practices and procedures (e.g. Performance Appraisals) must be avoided: including any that are unfairly critical of employees, students, parents, governors, directors or any other member of the Trust Community.

5.5.7 Emails received from those who are external to the Trust are to be treated in the same way as letters. A response should be sent within a reasonable period of time, usually within 48 hours of receipt.

5.5.8 If an email includes material that is confidential, a user who receives it must ensure that the necessary steps are taken to protect this confidentiality.

5.5.9 Users who are absent from work must use the 'Out of Office' function of the email system to indicate who will deal with your emails in their absence, and to specify their date of return to work.

5.6 Email contracts

5.6.1 Offers or acceptances transmitted via email can be equally legally binding as those sent on paper and so the same levels of diligence must be applied as would be if documentation was being sent in hard copy.

5.7 Information to be included in emails

5.7.1 Where a standard disclaimer or similar message has been made available users must ensure that their outgoing emails contain a copy of this.

5.8 Attachments

5.81. Employees must not attach any files to emails that may contain a virus. If the authorship of a file is not known it should be assumed unsafe to send as an attachment.

5.8.2 If a file is a programme (or executable file, e.g. one ending '.exe' or similar) it should never be sent by email without first checking with the IT department.

5.8.3 Employees should exercise care when opening attachments. In particular employees must not open attachments contained within emails received from third parties who are not known to the recipient user or who do not identify themselves.

5.9 Unsolicited emails

5.9.1 Emails that offer products or services, or 'junk' emails may be deleted or filed in an appropriate folder on the email system.

5.9.2 Other unsolicited emails that contain concerning material, particularly those that are sexually explicit, discriminatory or otherwise offensive, should be reported to the Headteacher immediately.

5.9.3 Instant messaging software may not be used on ICT without the manager or Headteacher's consent.

6. USE OF THE INTERNET

6.1 Where users are permitted to access the internet they must do so sensibly, appropriately and in such a manner that it does not interfere with the efficient running of the Trust.

6.2 Users may be asked to justify the amount of time they have spent on the internet or the sites that they have visited.

6.3 Users are trusted to use the internet sensibly and understand that when visiting an internet site, information identifying your PC may be logged. Accordingly activities may affect BET.

6.4 Whenever a user accesses a website, they must comply with any terms and conditions that govern its use.

6.5 Files may only be downloaded and/or saved to the Trust's system if this is expressly permitted by the terms of the internet site that holds this data.

7. **UNAUTHORISED USE OF THE INTERNET**

7.1 BET will not tolerate the use of its email or internet systems in any of the following:

- Any message that could constitute bullying or harassment;
- The circulation or exchange of messages or pictures that are inappropriate, offensive, obscene, illegal, defamatory, threatening, discriminatory, sexist or contain racist terminology or nudity, or infringes others' intellectual property rights, or which are intended to annoy, offend, harass or intimidate another person;
- Personal use such as social invitations, personal messages, jokes, cartoons or chain letters;

- Online gambling;
- The use of computer games at any time during working hours including breaks;
- Accessing pornography;
- Downloading or distributing copyright information and/or any software;
- Posting confidential information about the Trust, its employees, students, parents, governors, directors, clients, suppliers or any other member of the Trust community;
- Any illegal activity

7.2 Users must not:

- Use any images, text or material which are copyright-protected, other than in accordance with the terms of any licence under which they were permitted to download them;
- Seek to gain access restricted areas of the Trust's network;
- Access or try to access data which they know, or ought to know, is confidential;
- Introduce any form of computer virus, packet sniffing, password detecting software or other malicious code onto the ICT;
- Carry out any hacking activities;
- Carry out any activities that may be considered cyber bullying.

8. PERSONAL USE OF THE INTERNET/EMAIL

8.1 Although ICT is primarily for work use, BET understands that users may, on occasions, need to send or receive personal emails using their work address or access the internet for their own personal use. This is permitted on the following conditions:

- All the procedures and rules set out in this policy must be complied with;
- The number of personal emails is kept to a minimum and does not interfere with or take priority over work duties or responsibilities;
- Users who make personal use of the Trust's ICT consent to monitoring (see below);
- Time spent on personal emails or internet usage is confined to break times;
- When sending personal emails, users should show the same care as when sending work related emails;
- The internet is not used to access offensive, inappropriate or illegal material, such as material containing racist terminology or nudity or other 'banned' activities as listed under 'unauthorised use' within this policy;
- Employees do not enter into any contracts or commitments in the name of, or on behalf of the Trust;
- Employees do not arrange for any goods ordered on the internet to be delivered to the Trust's address or order them in BET's name;
- Users must not provide their work email address when using websites for non-work purposes;
- Users must not provide their work email address when using websites for non-work purposes;
- Users are responsible for informing anyone who emails in a private capacity that they must do so responsibly;
- Emails marked 'private' may be monitored by the Trust.

8.2 Users must not:

- Send the Trust's files or documentation to personal email addresses unless this is specifically for work purposes and has been agreed with the prior permission of a manager;

- Send or knowingly receive large email attachments (more than 10mb);
- Send or knowingly receive jokes, chain emails, images or similar.

9. GENERAL PROVISIONS

9.1 The Trust may deny any user access to ICT and/or revoke or remove authority to access the internet or make personal use of the Trust's email and/or internet systems.

9.2 Many sites that could be useful for the Trust require registration. A user who wishes to register must first obtain a manager's consent.

9.3 Some websites require the Trust to enter into licence or contract terms. The terms should be printed off and sent for approval by a manager or the Headteacher before they are agreed.

9.4 Users must evaluate whether or not information made available online is from a reputable source and is likely to be accurate and up-to-date. Users must avoid using any information that is not from a reliable and credible source and which is not known to be up to date and accurate.

9.5 users should only download files using computers equipped with virus checking software and should check how long the download will take.

9.6 If there is any uncertainty as to whether the item is virus-free or the time the download will take is reasonable, a manager must be consulted.

10. MONITORING AND INTERCEPTION OF ELECTRONIC COMMUNICATIONS

10.1 The Trust may access and monitor the use of any ICT. This may include but is not limited to monitoring file downloads and reviewing server and workstation file contents.

10.2 For the purposes of maintaining personal privacy, users need to be aware that such monitoring might reveal sensitive personal data. By carrying out activities users consent to the processing of any sensitive personal data that may be revealed by such monitoring.

10.3 The Trust may monitor the use of ICT for any reason including:

- Ensuring that the Trust's procedures, policies and contracts with employees are adhered to;
- Investigating or detecting unauthorized use of ICT;
- Ensuring the smooth running of BET's functions during a user's absence;
- Suspicions that an employee has been using the email system to send and receive an excessive number of personal communications
- Suspicions that an employee has been viewing inappropriate, offensive or illegal material, such as material containing racist terminology or nudity;
- Concerns that an employee has been spending an excessive amount of time viewing websites that are not work related;
- Preventing or detecting unauthorized use of the Trust's communications systems or criminal activities;
- Complying with any legal obligations;
- Monitoring standards of service and employee performance;
- Maintaining the effective operation of the Trust's communication systems;
- Ensuring compliance with any regulatory requirements;
- Preventing or detecting the commission of any criminal offence.

10.4 BET's reasons for needing to monitor are summarised below:

- BET is ultimately responsible for all communications. Therefore communications should not be considered to be private for the purposes of monitoring or otherwise;
- The Trust may intercept communications where it is believed that it is necessary to do so and can be justified within the provisions of the Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000;
- Wherever users use ICT for personal purposes they are notified of and consent to monitoring (see above);
- Any negative effect on a user's private life can be avoided by that person choosing not to use Trust ICT in the conduct of their personal affairs;
- To ensure compliance with this policy and any other rules that relate to the use of ICT;
- There are no suitable and less intrusive methods to effectively ensure proper and full compliance with this policy.

11. USE OF ICT EQUIPMENT IN THE CLASSROOM

11.1 During lesson delivery, a user who is the classroom teacher is fully responsible for all ICT equipment that is being used by their classes.

11.2 The user must ensure that ICT is used in compliance with this policy.

11.3 If a student has acted in a way that is a breach of this policy this must be reported to a manager or the Headteacher without delay.

12. DISCIPLINARY REGULATIONS AND ENFORCEMENT

12.1 Where a breach of this policy is alleged or a complaint received, this may lead to an investigation and thereafter result in disciplinary action.

12.2 Where a breach of this policy is alleged or found to have taken place, the user's access to ICT may be suspended temporarily or permanently as may be appropriate.

12.3 The Trust may refer a user to the police where appropriate and will co-operate fully with investigations.

13. WORKING REMOTELY

13.1 When ICT is used away from BET premises, or a user uses other equipment to undertake work related duties or functions away from the Trust premises, or a user uses other equipment to undertake work related duties or functions away from the Trust premises (working remotely), the user must:

- Password protect any work which relates to Trust business so that no other person can access it;
- Position themselves so that their work cannot be overlooked by any other person;
- Take reasonable precautions to safeguard the security of the ICT equipment and access to it;
- Inform the police and a manager as soon as possible if the ICT has been stolen and;
- Ensure that any work undertaken remotely is saved onto the Trust's system or is backed up and transferred to the Trust system as soon as possible.

Review frequency: 3 years
Review date: April 2020
Last updated: April 2017