Bourne Education Trust Staff Information, Communication & Technology (ICT) Policy

Throughout this document, the term 'staff' refers to anyone directly or indirectly employed by or working in a voluntary capacity in the Bourne Education Trust or in any of its schools.

Purpose

ICT and related technologies such as Email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the BET Head of ICT and/or Designated Safeguarding Lead for your school.

This policy reflects the BET values and ideas in relation to the safe teaching and learning of and with ICT. It sets out a framework within which teaching and non-teaching staff can utilise ICT equipment as part of their daily activities.

This document is intended for all staff.

Introduction

ICT is changing the lives of everyone. Our vision is for all members of the BET community to become confident users of ICT so that they can develop the skills, knowledge and understanding which enable them to use appropriate ICT resources effectively as powerful tools for teaching and learning, or as appropriate for their role.

Virus Protection Procedures

In order to prevent the introduction of viruses or other forms of contamination into BET schools' IT systems, the following must be observed:

a) unauthorised software including public domain software, magazine cover disks/CDs or Internet/World Wide Web downloads must not be used; and
b) all software must be virus checked using standard testing procedures before being used.

Use of Computer Equipment

In order to control the use of a school's computer equipment and reduce the risk of contamination the following will apply:

a) the introduction of new software must first of all be checked and authorised by the Head of ICT before general use will be permitted;
b) only authorised software may be used on any of the school's computer equipment;
c) only software that is used for teaching, learning and other official school applications may be used;
d) no software or hardware may purchased without prior authorisation by the school's Head of IT, or by a member of the trust's central IT team;
e) unauthorised copying and/or removal of computer equipment/software will result in disciplinary action.

Email and internet Policy

1. Introduction

   The purpose of the internet and email policy is to provide a framework to ensure that there is continuity of procedures in the usage of internet and email within each school. Use of the internet and email have established themselves as an important communications facility within the school and have provided us with contact with professional and academic sources throughout the world. Therefore, to ensure that we are able to utilise these systems to their optimum we have devised a policy that provides maximum use of the facilities whilst ensuring compliance with the legislation throughout.

2. Internet

   Where appropriate, staff are encouraged to make use of the internet as part of their official and professional activities. Attention must be paid to ensuring that published information has relevance to normal professional activities before material is released in the school's name. Where personal views are expressed a disclaimer stating that this is the case should be clearly added to all correspondence. The intellectual property right and copyright must not be compromised when publishing on the internet. The availability and variety of information on the Internet has meant that it can be used to obtain material reasonably considered to be offensive. The use of the internet to access and/or distribute any kind of offensive material, or material that is not work-related, leaves an individual liable to disciplinary action which could lead to dismissal.

3. Procedures – Acceptable/Unacceptable Use

   a) unauthorised or inappropriate use of the internet may result in disciplinary action which could result in summary dismissal;
   b) the internet is available for legitimate school use and matters concerned directly with the job being done. Staff using the internet should give particular attention to the following points:

      i) access during working hours should be for work use only;
      ii) private use of the internet should only occur outside of your normal working hours, except as outlined in the Code of Conduct.

c) the School will not tolerate the use of the internet for unofficial or inappropriate purposes, including:

   i) accessing websites which put our internet at risk of (including but not limited to) viruses, compromising our copyright or intellectual property rights;
   ii) non-compliance with our social networking policy;
   iii) connecting, posting or downloading any information unrelated to their employment and in particular pornographic or other offensive material;
   iv) engaging in computer hacking and other related activities, or attempting to disable or compromise security of information contained on the School's computers.

You are reminded that such activities (iii. and iv.) may constitute a criminal offence.

4. Email

The use of email is encouraged as its appropriate use facilitates efficiency. Used correctly it is a facility that is of assistance to staff. Inappropriate use however causes many problems including distractions, time wasting and legal claims. The procedure sets out the schools' position on the correct use of email.

5. Procedures - Authorised Use

a) unauthorised or inappropriate use of email may result in disciplinary action which could include summary dismissal;
b) Email is available for communication and matters directly concerned with the teaching and learning of students and the requirements of the school. Staff using email should give particular attention to the following points:

   i) Comply with the Code of Conduct and the Social Media policies;
   ii) Email messages and copies should only be sent to those for whom they are particularly relevant;
   iii) Email should not be used as a substitute for face-to-face communication or telephone contact. Flame mails (i.e. emails that are abusive) must not be sent. Hasty messages sent without proper consideration can cause upset, concern or misunderstanding;
   iv) if email is confidential the user must ensure that the necessary steps are taken to protect confidentiality. The school will be liable for infringing copyright or any defamatory information that is circulated either within the school or to external users of the system, and for any loss of personal data;
   v) offers or contracts transmitted by email are as legally binding on the school as those sent on paper.

c) The school will not tolerate the use of email for unofficial or inappropriate purposes, including:

   i) any messages that could constitute bullying, harassment or other detriment;

ii) personal use (e.g. social invitations, personal messages, jokes, cartoons, chain letters or other private matters);
iii) on-line gambling;
iv) accessing or transmitting pornography;
v) transmitting copyright information and/or any software available to the user; or
vi) sending any confidential information about other staff, the school or its students that is not directly relevant to the sender's job role

6. Monitoring

We reserve the right to monitor all email/internet activity by you for the purposes of ensuring compliance with our policies and procedures and of ensuring compliance with the relevant regulatory requirements and you hereby consent to such monitoring. This includes monitoring of any additional accounts you may be requested to set up for the purposes of performing your work tasks, which are subject to the same rules as your work email account. Information acquired through such monitoring may be used as evidence in disciplinary proceedings.

Social Networking

Any work related issue or material that could identify an individual who is a student, their parents/guardians or work colleague, which could adversely affect the school, a student, their parents/guardians or our relationship with any students, their parents/guardians must not be placed on a social networking site. This means that work related matters must not be placed on any such site at any time either during or outside of working hours and includes access via any computer equipment, mobile phone or other device.

On social networking sites you must not 'friend' a pupil or ex-pupil who is still a minor and will only 'friend' an ex-pupil over the age of eighteen if you meet them in an 'equal social setting'. You will not use social networking sites to discuss matters related to the school.

Any work content or material, or contacts or connections list, created by you during the course of your employment, on any of your authorised social networking sites (ownership of which vests in the school) shall remain, at all times, the property of the school. Accordingly, upon termination of your employment, you shall hand over to the school, the access rights to your accounts, together with any work content or material, and any contacts or connections list.

Passwords

All staff who have access to the school's computer systems are given usernames and passwords. You should keep your passwords confidential, change them regularly and do not under any circumstances give your password to a student or any other member of staff. When leaving your computer unattended, or on leaving the school, you should make sure that you log off, or lock the computer to prevent access in your absence. On termination of your employment for any reason, you must ensure that you notify the school of all access passwords.

Mobile Phones and Other Electronic Devices

Digital devices with cameras are now commonplace. A built in digital camera on a mobile device enables users to take high quality pictures which can then be sent instantly to other mobile devices or e-mail addresses. They can also be posted on the internet. There is the potential for such mobile devices to be misused in schools. They can become an instrument of bullying or harassment directed against pupils and teachers.

Use of personal mobile devices by staff during their working school day is at the discretion of each Headteacher, and if allowed, should be discreet and appropriate e.g. not in the presence of pupils.

Staff should never contact pupils or parents from their personal mobile device, or give their mobile device number to pupils or parents.

Staff should never send to, or accept from, colleagues or pupils, texts or images that could be viewed as inappropriate. No member of staff should ever use their personal device to photograph a pupil(s), or allow themselves to be photographed by a pupil. This guidance should be seen as a safeguard for members of staff and the school. Images for official school business, such as for use on a social media platform, must only be taken on a school-owned device, and must only be taken with the prior permission of the Headteacher and/or DSL. Each school should make such devices available for staff use, and monitor their use.

Staff should understand that failure to comply with the policy is likely to result in disciplinary action being taken.

Appendices
A - Acceptable Use Agreement/code of Conduct

Date Drafted:	**July 2014**
Approved by the Trust:	**September 2017**
Date Reviewed:	**April 2020**

Appendix A

Staff, Governor and Visitor Acceptable Use Agreement

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. All staff , Governors and visitors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the BET Head of ICT and/or DSL.

1. I will only use the school's email / internet / intranet / learning platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the BET in line with relevant policies and the Code of Conduct.

2. I will comply with the ICT system security and not disclose any passwords provided to me by the School or other related authorities, other than on termination of my employment, or on completion of my relationship with the school.

3. I will ensure that all electronic communications with pupils and staff are compatible with my professional role and are in line with relevant policies and the Code of Conduct.

4. I will only use the approved, secure email system(s) for any school business.

5. I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head teacher or the local Governing Body, and only in an approved manner.

6. I will not install any hardware or software on school-owned devices without permission from the Head of IT.

7. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory whilst on school premises, or whilst using a school-owned device

8. Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with BET policy and with written consent of the parent, carer (or student if aged 13+) or staff member. Persons taking photos of pupils or staff will have explicit permission from the Headteacher and DSL to do so. Images will not be distributed outside the school network without the permission of the parent/carer (or student if aged 13+), member of staff or Headteacher. See 'Mobile phones and other electronic devices' above.

9. I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.

10. I will respect copyright and intellectual property rights.

11. I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

12. I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature: I agree to follow this Acceptable Use Agreement and to support the safe use of ICT throughout the school.

Signature …….…… Date ……

Full Name …….. (printed)

Job title . . . .

BET ICT and Communication Policy CV-19 Appendix B

Addendum Applicable During Coronavirus (Covid 19) Period of Partial School Closures

This addendum is for the period of partial school closures imposed by the Government during the Coronavirus (Covid 19) outbreak only. Any additions or amendments listed should not in any way override or diminish an individual's responsibility to safeguard children and to act in an appropriate and professional manner at all times.

Where no exceptions and amendments are stated below then it should be understood that the expectations set out in the main body of this policy and in the Acceptable Use Agreement still wholly apply.

In school

We will continue to have appropriate filtering and monitoring systems in place in across all schools and centrally within the Bourne Education Trust.

IT staff will available to advise staff and are continuing to monitor the systems daily. Any concerns will be passed on to the Designated Safeguarding Lead (DSL) or their nominated substitute as per our Safeguarding policy Covid 19 addendum.

Outside school

Staff should be aware that school-owned devices used in the home setting may be subject to monitoring and access to inappropriate websites or engaging in inappropriate online behaviour remains a disciplinary matter.

Where staff are interacting with pupils online, they will continue to follow the existing IT Acceptable Use Agreement, the amended Staff Code of Conduct and the amended Safeguarding Policy. In these policies, clear guidelines are set out for the safe use of school IT equipment and the school network in relation to communicating with pupils and appropriate use of language. Only in exceptional circumstances, pre-approved by the Headteacher, is it appropriate for staff to livestream or videoconference with pupils in real time. Further guidance is available in a separate document.

As per this policy, staff continue to be prohibited from using social networking sites or apps to communicate with pupils, other than sites or apps approved by the Headteacher and BET central IT team and used to communicate with the whole school or parent community.

Any professional communications whether sent from a school or personal device in the course of a member of staff's duties may be used as evidence should any disciplinary procedures commence as a result of breaches of this or any other policy.

Pupils are unlikely to be using a filtered internet connection at home, so staff should be alert to signs that pupils may be making inappropriate use of the internet through comments they make or posts they share. Any concerns should be shared with the DSL in the usual way.

Pupils know how to report any concerns they have back to their respective school via dsl@jubileehigh.surrey.sch.uk

Pupils have already been signposted to welfare and well-being sources of support such as those on the Covid19 tab on the school website:

Working with parents and carers

We will make sure parents and carers:

- Are aware of the potential risks to children online and the importance of staying safe online
- Know what our schools are asking children to do online, including what sites they will be using and who they will be interacting with.
- Know where else they can go for support to keep their children safe online

Throughout the closure, regular updates will be offered to parents including links to relevant websites / media for further guidance.

Email and Internet Use

We appreciate that we are operating in extraordinary times where many members of staff will often be working from home and may be using their own devices for contacting pupils but staff should be reminded that all clauses of our Email and Internet Policy still apply when engaged in any communication with pupils, colleagues, parents and other stakeholders.

Staff are reminded that all aspects of GDPR and the Data Protection Act 2018 apply. Please pay particular attention to emails and other forms of communications and make sure:

- they are only sent to intended recipients
- they are purposeful and professional
- any emails addressed to multiple recipients use the BCC function so that, for example, parents' email addresses are hidden. Ideally, communications sent to multiple recipients such as a tutor group or year group will be sent by such proprietary methods as SchoolComms, ParentMail or similar as these systems automatically mask recipients' email addresses
- At no time should any school business be conducted using a personal email address.

Other GDPR and professional conduct points to be reiterated at this time include:

- Staff may have access to special category personal data about pupils and their families which must be kept confidential at all times and only shared when legally permissible to

do so and in the interest of the child. Records should only be shared with those who have a legitimate professional need to see them.

- Staff should never use confidential or personal information about a pupil or her/his family for their own, or others advantage (including that of partners, friends, relatives or other organisations). Information must never be used to intimidate, humiliate, or embarrass the child.

- Confidential information should never be used casually in conversation or shared with any person other than on a need-to-know basis. In circumstances where the pupil's identity does not need to be disclosed the information should be used anonymously.

- Communication with children both in the 'real' world and through web based and telecommunication interactions should take place within explicit professional boundaries.

Mobile Phones and Other Electronic Devices

If the use of a personal mobile device is unavoidable for contacting a parent/carer, then the number must be withheld, eg by typing 141 before dialling the parent/carer number. Staff personal mobile numbers should never be given to pupils or parents.

All email contact with pupils must be made using the member of staff's and the pupil's school email address, or through Microsoft Teams.

Any personally owned device used for school business must be protected by the minimum of a 4-digit PIN and/or biometric recognition. If the device is shared with other family members, the member of staff must log out of all school communication apps such as email, Teams, remote access or VPN systems.