BEDE'S

# Staff Acceptable Use Policy and Guidelines (Trust including EYFS)

## Related Policies

- E-Safety Pupil Acceptable Use Policy and Guidelines
- E-Safety Staff Acceptable Use Policy and Guidelines
- Keeping Children Safe in Education (2018)
- Taking, Storing and Using Images of Children Policy
- Staff Code of Conduct

## 1. Introduction

I. With computers and emerging technology becoming an integral part of our daily lives this policy should serve to ensure its safe and effective use. The Trust has provided a comprehensive ICT network and hardware for Staff to use primarily for educational and operational purposes, but also on occasion for personal use. All users should ensure that these systems are used responsibly and the Trust will therefore monitor the use of ICT systems, email and other digital communications.

II. Whilst the following may appear to highlight many "don’ts" or "risks" please be assured that we promote the enthusiastic use of the Trust’s ICT systems and infrastructure. However as 'global' systems and communication tools grant us 'instant access' and the ever-greater ability to connect and exchange information widely, we do have to recognise both the benefits and the potential 'risks'.

## 2. Equipment:

a) Equipment provided to staff by the Trust should be used and stored securely. Any loss must be reported immediately to the Head of IT Services
b) Mobile devices are particularly susceptible to theft and where appropriate precautions have not been taken, a replacement charge may be requested of the user. Appropriate precautions include but are not limited to:
    a. Not leaving the laptop or mobile device unattended, regardless of location
    b. Ensuring that the laptop or mobile device is not visible when leaving a motor vehicle (securely locked in the boot of the vehicle)
    c. Being particularly cautious in ‘public’ spaces
c) Any faults with Trust-provided equipment should be reported immediately to the IT Services department via helpdesk@bedes.org
d) All mobile devices (e.g. personal laptop, smart phone, tablet pc) must be scanned by the user and ensured to be virus free before connecting to the School network
e) Do not attempt to modify or remove any hardware maintained by the Trust unless authorised by the IT Services department to do so
f) The provision of equipment by the Trust is primarily for the use of School related business. Any personal use must be in accordance with the guidelines as laid out in this policy
g) The procurement of hardware, software or consumables (whether through departmental budgets or personal funds) can only be authorised by the Head of IT Services
h) Staff should under no circumstances connect personal equipment to the network via a hard wired connection.
i) Any personal equipment that is regularly used in School or left overnight must be PAT tested
    a. (arranged by contacting the Porters Lodge)

## 3. Personal and Professional Safety and Security

a) Users must never disclose their usernames or passwords (MIS and Network) to anybody
b) Similarly, it is not permissible under any circumstances to use another user's credentials to access the School network
c) No attempt should be made to alter security settings as this may put the network at risk
d) Whilst staff resources folder have limited permissions (e.g. access is limited only to certain individuals), there may be exceptional circumstances (holiday leave, sickness, disciplinary matters) when, for reasons of safeguarding, safety and/or the smooth running of the School, the Headmaster or Principal Deputy Headmaster consider it essential that staff files and electronic communication are accessed. The formal process will involve the following steps:

   a. A written request (via email or similar) from the Headmaster or Principal Deputy Headmaster or Prep School Deputy Head to the Head of IT Services to scrutinise staff School internet activity and/or files and/or emails for specific information

   b. If approved the of Head IT Services (or suitably appointed IT staff member) will gain access to the requested files, activity log or email folders and provide the required information, or a 'nil return' in the case of email boxes

e) In order to facilitate the smooth running of the Schools, access may be given to another member of staff (such as a line manager, departmental colleague or cover person) with permission from the Headmaster or Principal Deputy Headmaster or Deputy Head (Prep) to the Head of IT Services to access the above mentioned files and email.

## 4. Information and Data Security

a) Sensitive information should not be stored on a laptop or other mobile device for extended periods of time
b) If necessary, this data should be stored on the network (not on the physical drive which is local to that machine) and accessed via an approved web portal
c) Personal details of pupils including contact details should not be stored on a mobile device or removable media (e.g. memory stick)
d) Any device (School provided or personal) used to access Trust information **must** be password protected
e) Pupils should under no circumstances be granted unattended access to staff workstations (e.g. offices, classrooms) and staff must lock workstations devices when unattended

## 5. Email and Internet

I. Whilst access to the Internet is provided primarily for educational and operational uses, the Trust recognises that there are times when residential and non – residential staff may need to use the Internet and School email systems for personal use. However, this should never disrupt staff duties. Any online activity should in no way compromise your professional responsibility or bring the Trust into disrepute. Any abuse or excessive personal use of email and or Internet facilities will be dealt with through the disciplinary procedure.

### a) Email

a) The use of Bede's email has been provided for the sole purpose of communication with colleagues, pupils, parents and School-related external parties. Personal email accounts should be used for all personal communication
b) Staff should not use their own personal email accounts to communicate with pupils

c) Communication via email should at all times be in a polite and professional manner and should not be of an aggressive or inappropriate tone and should not contain offensive, aggressive or inappropriate language

d) The attachment and transmission of inappropriate, obscene, unlawful or abusive material is not acceptable under any circumstances

e) Staff should immediately report any inappropriate emails to the of IT Services or their Line manager

### b) Internet

a) Using the Internet/network to obtain, send, store, print, display or transmit material, which is obscene, abusive or unlawful, will not be tolerated

b) Users must at all times respect the ownership rights of materials and abide by copyright laws

c) This includes accessing, copying, altering, removing or uploading files owned by other users

d) Staff should remain polite when communicating with others and shall not use strong, aggressive, insensitive or inappropriate language

e) To ensure the safety of users, the Trust may monitor the use of ICT systems including email and other digital communication

f) Limited personal use (e.g. Holiday booking, Internet Banking) is permissible during break, lunch or free periods

g) File sharing / peer-to-peer networking is prohibited on the network

h) The use of media streaming websites (e.g. YouTube, Iplayer) is restricted to School-related purposes

i) Staff should not use third party software or other means to circumnavigate filtering and or security features of the network

### c) Social Media and Networking Sites

I. Social media and networking sites as referred to in this policy, are any internet related platforms whereby messages, information (which includes images, video or text) can be communicated to an audience both publically or as part of a closed group.

II. Examples of commonly used social media and networking platforms are include: Twitter, Facebook, Instagram, Google Docs, multiplayer online games, forums and online bulletin boards.

## 6. Creation of Social Media accounts:

a) The use of a House, Department or Subject specific account should be strictly for the dissemination of educational, marketing or subject based information.

b) If staff choose to make use of social networking sites for School purposes, personal details such as private email addresses, home addresses or mobile numbers which could identify themselves and their location, should never be distributed or be on public display, and must avoid any risk of pupils being able to contact staff outside of the School environment.

c) All accounts should be setup using Bede's email addresses example@bedes.org and not use a personal email account. Where this is not possible, permission must be obtained from the Principal Deputy Headmaster.

d) The full URL, master password, associated email address and the name of all social media accounts and networking sites should be lodged with the **e-Safety co-ordinator** for inclusion in the Central Register of Social Media pages.

e) The names of all staff members with access to such accounts should be included when registering the details of the account.

f) No personal details such as private email addresses or mobile numbers of any staff members should be made available or accessible through this account.

g) The account name should be set up on a House, Department or sports basis and no member of staff should be identifiable or associated with this name in any way e.g. Deis.Twitter@bedes.org

h) The account must be branded in-line with other Bede's public facing accounts, the account should be passed for approval by the Marketing Team.

i) The biography section of the account (if applicable) should be filled in using only House, Department or subject based information.

j) The account must be for "broadcast" only and any followers or readers should not have the ability to post directly or reply to any threads on the account. The facility for "commenting on", "replying to" or "direct messaging" should be disabled at the time of account creation unless agreed by the Principal Deputy Headmaster.

k) Staff should avoid individual pupil contact including contact with former pupils under the age of twenty-one which includes but is not limited to:

   a. Accepting "friend" requests
   b. Engaging in instant messaging or mobile text messaging conversations
   c. Replying to an online thread or message
   d. Replying to a wall post or commenting on an online forum
   e. Commenting on or tagging a photograph

l) Any attempt by a pupil, or former pupil under the age of twenty-one-years old, to make contact with a member of staff should be rejected and reported to the respective line-manager, e-Safety co-ordinator or Deputy Safeguarding Lead

m) Personal posts or comments should not bring the reputation of the Trust or any of its members into disrepute

I. The use of public facing media can have both a wholly positive and negative effect not only for the individual but also the Trust as a whole if used incorrectly. It is therefore imperative that staff making use of Social Media to disseminate information and keep this at the forefront of their minds when posting, reposting or commenting on topics, the following points should be noted:

## 7. Guidelines:

a) Posts should always be of an educational and marketing nature

b) The appropriate copyright laws should be adhered to at all times and similarly any intellectual property rights should be respected at all times

c) All posts or links to articles that are re-posted should be read thoroughly to ascertain their appropriateness for the intended audience

d) No personal views or messages should be expressed through this medium

e) Language should remain professional at all times

f) Media which include images of pupils (for example on a field trip) should only be posted online with pupils' permission following the same guidelines regarding the use of digital images as with other websites and publications

g) Pupils should only be referred to by name if permission has been granted

h) The personal and professional boundary shall be retained at all times

i) Nominated staff members are at all times responsible for the content that appears on the relevant Social Media account

j) All Social media accounts are subject to regular auditing and scrutiny and if it is felt by the Senior Management Team that the effectiveness or suitability of any account is not of an educational or marketing benefit or if the Trust or any of its members are brought into disrepute, a request will be made for the immediate removal of the account in question

k) Understand that this Policy applies not only to professional conduct and related work within the Trust, but it also applies to the use of the Trust ICT systems and equipment outside of the Trust and use of personal equipment or in situations related to employment by the Trust

l) Understand that failure to comply with this agreement, could lead to disciplinary action. This would be in accordance with the Trust's disciplinary procedure and, in the event of illegal activities, the involvement of the police

### d) Mobile Devices, Digital Content, images and video

I. As part of the contractual obligation between parents of a pupil and the Trust. It is agreed that photographs and or moving images may be taken and used by the Trust in accordance with normal custom and practice. Such custom and practice will include: set piece photographs of the School, house, team, theatre cast and snapshots of School activities. Any use of images of pupils for marketing purposes, such as in prospectuses and promotional videos or displays on its website, inclusion in newsletters or publication in local media must only be done after appropriate consent has been acquired.

II. All staff must ensure that all photographs and videos are published in line with the School's "Taking, Storing and Using Images of Children Policy" and that the appropriate consent has been given.

III. The terms and conditions of Admission specify that parents who do not want their child's photograph or image to appear in any of the Trust's promotional material must make sure that their child knows this and have clearly stated this by not consenting on the Trust's Terms and Conditions form.

### 8. Equipment

I. Images / video should be taken using Trust supplied equipment.

II. Personal equipment should not be used for digital imagery **unless** a Trust provided removable media (memory card) is used, **or** permission has been obtained to use a personal device (see guidance regarding storage below).

III. No device should ever be used for any recording purposes in changing rooms, bedroom accommodation, bathrooms or any cloakroom facility.

### 9. Storage

I. Images should be stored on a secure password protected area of the School network and never held on personal equipment for longer than necessary before transfer to the School network e.g. the same day, or within a three days.

II. If personal storage devices have been used to transfer images / video these should be deleted once transferred onto the School network.

III. Images should never be stored on personal devices which includes but is not limited to (mobile devices, laptops, internal camera memory, memory sticks or portable hard drives).

### 10. Publication

I. Digital content that is to be published in either digital or hard copy platforms should be selected carefully and passed for publication by the Marketing Department or relevant line manager prior to publication (e.g. Housemaster in the case of pastoral specific publications).

II. Should a pupil wish to create an image / video of another pupil for use or as part of GCSE or A –Level coursework, the teacher concerned should obtain written permission from the respective parent(s) and student. A thorough brief as to the nature and context of the image / video should be supplied to the teacher for approval prior to commencement of any photography / filming. This consent should then be passed logged with the e-Safety Coordinator.

III. Such images should be stored securely and should be deleted upon completion of the project.

IV. Any image should be screened by the teacher concerned prior to public display or submission to an examining body.

## 11. Context

I. When taking digital images / video, the emphasis should always be for educational, marketing or reporting aims.

II. Care should be taken when taking digital images / video that pupils are appropriately dressed and are not participating in activities that might bring the School or other individuals into disrepute.

III. Staff should ensure that if the image / video is viewed out of context that it will not reflect negatively on either the Trust or the individual.

## 12. Child Protection:

I. Staff should remain vigilant and report any of the following concerns to the Designated Safeguarding Lead should they become aware of anybody who is:

a) Taking images in inappropriate locations (toilets, changing or cloakroom areas)
b) Taking unusually large number of images
c) Taking images where the subject(s) are unaware that they are being filmed or photographed

II. Staff should ensure that they only access the School's pastoral system in a secure and confidential environment in line with the School's 'OOPS' policy:

**O**verlooked - *Be alert to your surroundings making sure that you are not overlooked or projecting your computer screen onto other devices*
**O**bjective - *Explain clearly detailing any specific evidence which you have been made party to*
**P**unctual – *Report this information in a timely fashion to ensure that it is as accurate as possible*
**S**ensitive - *Remember that this information is highly sensitive*

## 13. Taking of Images by parents and friends:

I. Parents and friends often wish to take images of their children at School plays and concerts or sporting activities. Courtesy and good manners require that the following rules are respected:

a) Visitors must use their cameras with consideration and confine their photography to the relevant event;
b) If visitors ask whether they can take photographs, they should be reminded that whilst it is permissible under the General Data Protection Regulation and Data Protection Laws (2018) to take photographs for personal use, publication of such images may be unlawful;
c) Where a play or concert or other event is subject to copyright and performing rights restrictions, visitors will not be permitted to take images, photographs or video film.

## 14. Use of Images as part of pupil records:

I. Pupils will be required to have a photograph taken for personal pupil records and identity cards. These images are subject to the Data Protection Act 2018 and will therefore:

a) Be stored on the secure network provided area
b) Not be used for any other purpose without the permission of the pupil or their parent(s)
c) Not be distributed or shown to any unauthorised party

### 15. Request by third parties:

I. From time to time third parties may request still or moving images of pupils for external publication. Such requests shall be handled by the Marketing Department who will gain the necessary permission of the pupil or their parent(s).

II. Photography and filming by newspaper journalists or television film crews will only take place under supervision once authorised by the Director of Marketing or their appointed person. If published, pupils will only be named if deemed appropriate and necessary by the Director of Marketing.

### e) Mobile phone numbers and texting

I. Staff should not provide either their home or mobile phone numbers to pupils**.** Pupils' telephone numbers should not be stored on personal mobile telephones**.** Any digital communication with pupils should be limited to official Trust email or Trust mobile phones provided for a School related activity.

### f) Accountability agreement

I. I understand that this Acceptable Use Policy applies not only to my professional conduct and related work within the Trust, but it also applies to my use of the Trust ICT systems and equipment outside of the Trust and my use of personal equipment or in situations related to my employment by the Trust.

II. I understand that if I fail to comply with this Agreement, I could be subject to disciplinary action.
    a) This would be in accordance with the Trust's disciplinary procedure and in the event of illegal activities, the involvement of the police

| | |
|---|---|
| **Author:** | E-Safety Co-ordinator |
| **Owned by:** | Principal Deputy Head |
| **Authorised by:** | SMT |
| **Date:** | November 2018 |
| **Review Date:** | November 2019 |
| **Circulation:** | School website, All parents, All Staff, All Pupils |

Appendix 1

## EYFS Acceptable Use Policy Guidelines

These rules are a reflection of the content of the Trust's E-Safety Policy. It is important that teachers and parents/guardians read and discuss the following statements with their pupils, understanding and agreeing to follow the Trust's rules on using ICT, including use of the Internet.

a) I will ask a teacher (or suitable adult) if I want to use a computer
b) I will only use activities that a teacher (or suitable adult) has told or allowed me to use.
c) I will take care of the computer and other equipment
d) I will ask for help from a teacher (or suitable adult) if I am not sure what to do or if I
e) think I have done something wrong.
f) I will tell a teacher (or suitable adult) if I see something that upsets me on the screen.
g) I know that if I break the rules I might not be allowed to use a computer.