EAST BARNET SCHOOL "I want to learn"

# eSAFETY POLICY

Version 4.0

| | |
|---|---|
| Review by People Committee: | 15th September 2014 |
| Adopted by Governing Body: | 13th October 2014 |
| Next Full Review Due: | Autumn 2018 |
| | |
| Reviewer: | M Duraku |
| Governor Link: | Governor with responsibility for Safeguarding |

# eSAFETY POLICY

## East Barnet School, Chestnut Grove, East Barnet, EN4 8PU

## A. Introduction and Statement of Principle

East Barnet School recognises that ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of the school community and beyond. As a school, we have built in the use of e-technologies as a resource for learning and to equip our students with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. We must also recognise the constant and fast paced evolution of ICT within our society and make provision for it. Internet technologies which children and young people are currently using, both inside and outside of the classroom, include:

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

Whilst exciting and beneficial, both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. We must ensure that all users, including parents, need to be aware of the risks associated with the use of these Internet technologies and that some have minimum age requirements, usually 13 years.

At East Barnet School**,** we understand the responsibility to educate our students on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual; the school's eSafety Policy and linked 'ICT & Internet: Acceptable Use Policies' (ICT AUP) are designed to protect against and minimise the loss of sensitive information that may result in media coverage, and potentially, damage the reputation of the school and individuals.

We recognise that everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the ICT AUP for all staff, governors, visitors and students are inclusive of both fixed and mobile internet access; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies

owned by staff, governors or students, but brought onto school premises (such as laptops, mobile phones, and other mobile devices).

## B. Requirements

eSafety is complex and continually evolving; East Barnet School reserves the right to implement measures or take action at short notice in order to keep the school community safe. At all times any action taken will be done in accordance with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Regulations 2000.

1. **ICT & Internet: Acceptable Use Policy (ICT AUP)**
   All members of the school community who have access to school equipment or who use the school network or any ICT facility either in or outside of school must read and sign and be bound by an appropriate Acceptable Use Policy agreement. *See ICT & Internet: Acceptable Use Policy. Note: there are different versions for staff and students.*
2. **Monitoring**
   2.1. The Headteacher and authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice.
   2.2. Authorised ICT staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.
   2.3. Authorised ICT staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.
   2.4. Please note that personal communications using school ICT systems may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.
3. **Breaches of the ICT Acceptable Use Policy**
   3.1. A breach or suspected breach of the ICT AUP or eSafety Policy by a school employee, contractor or student may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual. (*See Managing an eSafety Incident - Appendix 1*)
   3.2. Any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, where appropriate, breaches may also lead to criminal or civil proceedings.
4. **Incident Reporting**
   4.1. Any breaches or attempted breaches of the eSafety Policy or ICT AUP; loss of equipment; and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's eSafety Co-ordinator (ESC), the Child Protection Officer (CPO), a member of the Senior Leadership Team or the Chair of the Governing Body as appropriate.
   4.2. All security breaches, lost/stolen equipment or data (including remote access and passwords- PINs), virus notifications, unsolicited or 'suspect' emails and all other policy non-compliance must be reported to the ESC or directly to the IT Dept.
5. **Computer Viruses**

5.1. All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick, must be checked for any viruses using school provided anti-virus software before being used.
5.2. Any anti-virus software installed on school ICT equipment that you use must not be tampered with under any circumstances.
5.3. Staff with an allocated school laptops, if not routinely connected to the school network, must make provision for regular virus updates each month by logging on the laptop in school.
5.4. If staff suspect there may be a virus on any school ICT equipment, it should be switched off and reported to the ICT Department immediately. The ICT Department will advise what actions to take and be responsible for advising others that need to know.

**6. Email**

The use of e-mail within most schools is an essential means of communication for both staff and students.

6.1. In the context of school, e-mail should not be considered private.
6.2. The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.
6.3. It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business.
6.4. Under no circumstances should staff contact students, parents or conduct any school business using personal e-mail addresses.
6.5. The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school'. The responsibility for adding this disclaimer lies with the account holder
6.6. All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
6.7. Staff should restrict the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.
6.8. Staff must inform the ESC or line manager if they receive an offensive e-mail.
6.9. When staff access school e-mail either directly or through webmail or on non-school hardware the school ICT AUP still applies.
6.10. When appropriate activate your 'out-of-office' notification when away for extended period.
6.11. E-mails created or received within a member of staff's role in school will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

**7. Emailing Personal, Sensitive, Confidential or Classified Information**

When data needs to be emailed staff must:

7.1. Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
7.1.1. Encrypt and password protect as appropriate.
7.1.2. Verify the details, including accurate e-mail address, of any intended recipient of the information.
7.1.3. Verify the details of a request or before responding to e-mail requests for information.
7.1.4. Not copy or forward the e-mail to any more recipients than is absolutely necessary.

7.1.5. Do not identify any confidential details in the subject line of the e-mail.

7.1.6. Do request confirmation of safe receipt.

**8. eSafety Roles and Responsibilities**

8.1. Staff, Governors and Students must be made aware of which members of staff are the named eSafety Co-ordinator and Child Protection Officer.

8.2. Part of the roles of the ESC and CPO is to keep up to date with current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet.

8.3. The SLT and governors are updated by the ESC and CPO and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

8.4. This policy, supported by the school's Acceptable Use Policy for staff, governors, visitors and students, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: Child Protection, Health and Safety, Home–School agreements, and the Behaviour and Anti-Bullying Policy and PSHEE curriculum.

**9. E-safety: the Curriculum and the Community**

*9.1.* ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to the students and the wider school community on a regular and meaningful basis and we continually look for new opportunities to promote e-Safety without being alarmist or over-reactive. Students, parents and staff are alerted, not only to the dangers of the internet but also how to report abuse and where to seek help and advice. (*See: eSafety: Supporting/Educating Students - Appendix 2*)

9.2. We promote e-safety in a number of ways:

9.2.1. e-Safety is embedded within our ICT curriculum and, where applicable, in other curriculum areas.

9.2.2. As part of Child Protection training staff are updated as to the latest guidance on keeping students and themselves safe.

9.2.3. New staff receive information and sign the AUP as part of their induction.

9.2.4. Extended assemblies and workshops to students and evening presentations to parents on the subject of e-safety form part of our commitment to e-Safety.

**10. Internet Access and Management**

10.1. The school provides students supervised access to internet resources through its fixed and mobile internet.

10.2. Staff will preview any recommended sites before use.

10.3. If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

10.4. If staff or students discover an unsuitable site, the screen must be switched off/ page closed and the incident reported immediately to the ESC/IT Dept. as appropriate.

10.5. The school uses management control tools for controlling and monitoring workstations.

10.6. All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

10.7. All users must observe copyright of materials from electronic resources.

10.8. As stated in the AUP staff or students must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience.

10.9. As stated in the AUP staff must not reveal names of colleagues, students any other confidential information acquired through their role in school on any social networking site.

10.10. It is at the Headteacher's discretion as to what internet activities are permissible for staff and students using school equipment or internet facility.

**11. Managing Other Web 2 Technologies**

*Web 2.0 (or Web 2) is the term for advanced Internet technology and applications including blogs, wikis, RSS (for distributing web content) and social bookmarking.*

As a school we recognise that Web 2 Technologies, including social networking sites, if used responsibly both outside and within an educational context, can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites. (*See the School's ICT + Internet Acceptable Use Policies)*

**12. Parental/ Carer Involvement**

We believe that it is essential for parents/carers to be fully involved with promoting e-Safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss e-Safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies together with the associated risks.

12.1. Parents/Carers and students are consulted when appropriate to contribute to the reviews of the school e-Safety policy and the AUP.

12.2. Parents/Carers are asked to read through and sign acceptable use agreements along with their child on admission to the school. The AUP contains the following statement: *We/I the parent(s)/Carer(s) of ____ will support East Barnet School's approach to on-line safety as outlined in the Acceptable Use Policy and will strive to ensure he/she does not deliberately upload or add any text, images, sounds or video or misuses any electronic device or any social network in a way that could upset or offend any member of the school community.*

12.3. Parents/Carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain e.g., on the school website (*See Parental Consent Form - Appendix 3*).

12.4. The school disseminates information to parents relating to e-Safety where appropriate in the form of:

E-safety Information and evenings
The fortnightly newsletter
The school website

**13. Password Security**

Password security is essential for staff, particularly as they are able to access and use student data. Staff are issued with secure passwords which are not shared with anyone. The students are expected to keep their passwords private and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.

13.1. Staff must enter personal passwords in order to logon.

13.2. Staff are reminded to change passwords whenever there is any indication of possible system or password compromise.

13.3. If staff are aware of a breach of security with passwords or an account they must inform the IT Department immediately.

13.4. Passwords or encryption keys should not be recorded on paper or in an unprotected file.

13.5. Personal passwords will only be shared with authorised ICT support staff.

**14. Zombie Accounts**

A Zombie account refers to users who have left the school and therefore should have no access to the school's systems. If left active, these can represent a security threat by allowing unauthorised access.

14.1. Email accounts are 'locked' for a period of 12 months from the date a member of staff ceases to be employed by East Barnet School after which time the account is terminated.

**15. Safe use of Images**

Digital images are easy to capture, reproduce and publish and, therefore, misuse. East Barnet School is mindful that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

15.1. Students' names will not be published alongside their image and vice versa. E-mail and postal addresses of students will not be published. Students' full names will not be published.

15.2. If staff use personal digital equipment, such as mobile phones and cameras, to record images of students, for example on field trips, they must be transferred immediately and solely to the school's network and deleted from the staff device. No image can be uploaded onto social media without the Headteacher's expressed permission.

15.3. Students are not permitted to use personal digital equipment, including mobile phones and cameras to record images of others without expressed permission.

15.4. Permission must be sought from the Headteacher before any image of a student or member of staff can be uploaded for publication on the school's website.

**16. Publishing or Using Images of Students**

16.1. East Barnet School will always obtain the written consent of parents before using any image of a student (*See Parental Consent Form - Appendix 3*) in the following ways:

16.1.1. On the school web site.

16.1.2. In the school prospectus and other printed publications that the school may produce for promotional purposes.

16.1.3. Recorded/transmitted on a video or webcam.

16.1.4. On the school's learning platform or Virtual Learning Environment (VLE).

16.1.5. In display material that may be used in the school's communal areas.

16.1.6. In display material that may be used in external areas, i.e. exhibition promoting the school.

16.1.7. General media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

16.2. The consent for use of images form is considered valid for the entire period that the student attends this school unless there is a change in the family circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

16.3. In the case of parents no longer living in the same household, consent has to be given by both parents in order for it to be deemed valid.

16.4. Parents/Carers may withdraw permission, in writing, at any time.

**17. Publishing or Using Images of Members of Staff**

Permission will be sought from a member of staff to use their image as per sections 16.1.1-16.1.7

**18. Storage of Images**

Images/ films of students and staff are stored on the school's network.

18.1. Rights of access to this material are restricted to the teaching staff and students within the confines of the school network or online school resource.

18.2. Students and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher.

18.3. East Barnet School will securely archive all stored images when they are no longer required.

**19. Webcams and CCTV**

The school uses CCTV for security and safety. The only people with access to this are the Premises Team and the Senior Leadership Team.

19.1. We do not use publicly accessible webcams in school

19.2. Webcams in school are only ever used for specific learning purposes. Consent is sought from parents and staff on joining the school in the same way as for all other images.

## C. Related Policies and Documents

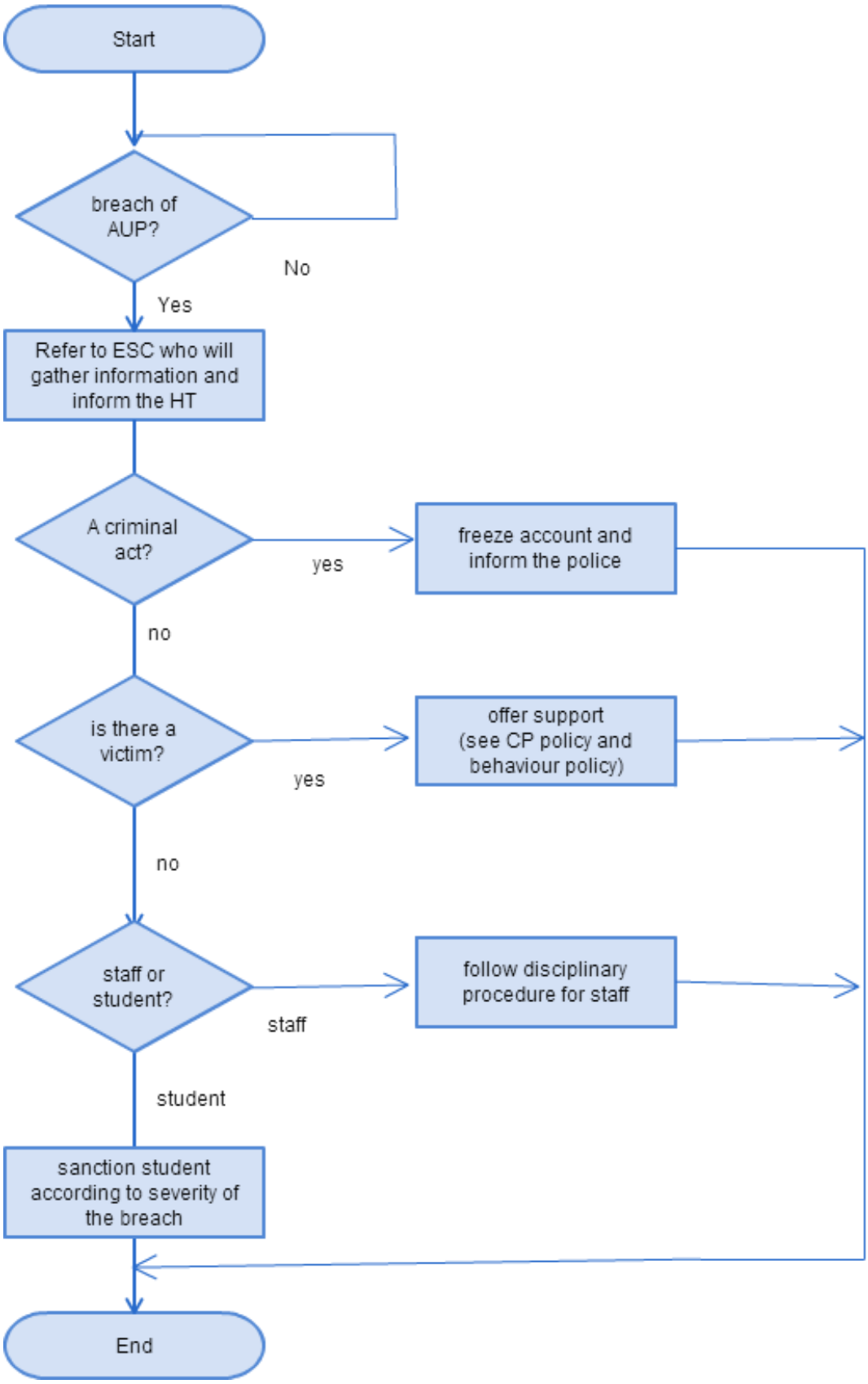
1. Behaviour Policy
2. ICT & Internet: Acceptable Use Policy a. Staff
3. ICT & Internet: Acceptable Use Policy b. Students
4. Information Policy (inc. Data Protection)

## D. Appendices

1. Managing an eSafety Incident
2. eSafety: Supporting/Educating Students
3. Use of Images Parental Consent Form.

## MANAGING AN E-SAFETY INCIDENT

**Appendix 1**



## eSAFETY: SUPPORTING/EDUCATING STUDENTS **Appendix 2**

1. At present, the school endeavours to deny access to social networking and online games website to students within school
2. All students are advised to be cautious about the information given by others on such websites, for example users not being who they say they are
3. Students are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
4. Students are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
5. Our students are advised to set and maintain online profiles to maximum privacy and deny access to unknown individuals
6. Students are encouraged to be wary about publishing specific and detailed private thoughts online
7. Our students are asked to report any incidents of cyber-bullying to the school their Head of Year or any adult within the school
8. Staff may only create blogs, wikis or other online areas in order to communicate with students using the school learning platform or other systems approved by the Headteacher

## USE OF IMAGES: PARENTAL CONSENT FORM

**Appendix 3**

**NAME OF STUDENT: …….....……..**

**Year & Form: ……..……**

Dear Parent/Guardian

Occasionally, we may take photographs of the children at our school. We may use these images in our school prospectus or in other printed publications that we produce, as well as on our website. We may also make video or webcam recordings for school-to-school conferences, monitoring or other educational use.

From time to time, our school may be visited by the media who will take photographs or film footage of a visiting dignitary or other high profile event. Pupils will often appear in these images, which may be published in local or national newspapers, or be used in television programmes.

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make any recordings of your child. Please answer the questions below, then sign and date the form where shown and return it to the school office.

Yours faithfully

**N Christou**
Headteacher

| | *Please circle your answer* |
|---|---|
| May we use your child's photograph in the school prospectus and other printed publications that we produce for promotional purposes? | Yes / No |
| May we use your child's image on our website? | Yes / No |
| May we record your child's image on video or webcam? | Yes / No |
| Are you happy for your child to appear in the media? | Yes / No |

***Please note that websites can be viewed throughout the world and not just in the United Kingdom where our law applies. Please note that the conditions for use of these photographs are on the back of this form.***

***I have read and understood the conditions of use on the back of this form.***

Full Name (Capitals) ……..

Signature : …… Date: ……

**CONDITIONS OF USE**

1. This form is valid for five years from the date you sign it, or for the period of time your child attends this school. The consent will automatically expire after this time.
2. Photographic images will be stored in the school archive and may at some future date be used by the school for display purposes only.
3. We will not re-use any recordings after your child leaves this school. The school will be responsible for securely storing all the photographic images (stills and video) at all times to prevent misuse, theft etc.
4. We will not use the personal details or full names (which means first name and surname) of any child or adult in a photographic image on video, on our website, in our school prospectus or in any of our other printed publications.
5. We will not include personal e-mail or postal addresses, or telephone or fax numbers on video, on our website, in our school prospectus or in any of our other printed publications.
6. If we use photographs of individual pupils, we will not use the name of that child to accompany the article.
7. If we name a pupil in the text, we will not use a photograph of that child to accompany the article.
8. We may include pictures of pupils and teachers that have been drawn by the pupils.
9. We may use group or class photographs or footage with very general labels, such as “a science lesson” or “making Christmas decorations”.
10. We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately

EAST BARNET SCHOOL "I want to learn"

# Acceptable Use Policy: Students

- I will only use ICT systems in school, including the internet, e-mail, digital video and mobile technologies, for school purposes.
- I will not download or install apps or other software on school computers or other devices.
- I will only log on to the school network, other systems and resources with my own user name and password.
- I will never tell anyone my password or allow anyone to use my school login.
- I will use my school e-mail address, and not a personal address, when sending email from school.
- I will not use personal social media accounts for school purposes.
- I will make sure that all ICT communications with students, teachers or others are responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not use ICT communications to promote or take part in cyber-racism.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidently come across any such material I will report it immediately to my teacher.
- I will only download music, images or videos in accordance with their licence agreements and only for the purposes of school work.
- I will not give out any personal information such as name, phone number or address. I will ensure that images of students or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed inside or outside the school network without permission.
- I will ensure that my online activity, both in school and outside school, will not cause East Barnet School, its staff, students or others distress or bring them into disrepute.

- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system, use hacking tools, or attempt to change any system settings.
- I understand that all my use of the Internet and other related technologies within school is monitored and logged by my teachers.
- I will use printers responsibly and will not needlessly waste paper. I will only use the schools' printers to print school work.
- If I am given permission to use my own tablet or laptop in the school, I agree that I will use it for the work allocated by the relevant member of staff.
- I understand that if I use my own device and a member of staff suspects I have not followed the rules regarding the use of my device, the member of staff will be allowed to inspect the contents of my device.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted.

I have read and understood the Acceptable Use Policy above

Signed _____ Date _____

Full Name (Capitals) _____

***We/I the parent(s)/Carer(s) of _____ will support East Barnet School's approach to on-line safety as outlined in the Acceptable Use Policy and will strive to ensure he/she does not deliberately upload or add any text, images, sounds or video or misuses any electronic device or any social network in a way that could upset or offend any member of the school community.***

Signed _____ Date _____

Signed_____ Date _____

Full Names _____ _____

# ICT Network and Internet Acceptable Use Policy: Staff

## East Barnet School, Chestnut Grove, East Barnet, EN4 8PU

---

This Acceptable Use Policy (AUP) is written in the form of an agreement between the school and each member of staff. A copy of the policy will be included on the school web site, on Fronter and in the staff information pack. Copies can also be obtained from the school office. The AUP will be reviewed annually.

### Aims

The aims of this Acceptable Use Policy are:

1. To ensure that staff benefit from the opportunities offered by the school's ICT resources in a safe and effective manner;
2. To provide and maintain ICT resources for the benefit of all staff and students;
3. To encourage staff to use these resources as an aid to effective execution of professional duties and responsibilities;
4. To protect the school's ICT infrastructure from misuse and attack;
5. To protect and securely maintain Sensitive and Personal Data.
6. To support the school's e-safety document.

### A. General

1. Observe good computer etiquette at all times and never undertake actions that may bring the school into disrepute.
2. Always log off at the end of your session so other people are not prevented from using the computer.
3. Use the school network and computers only for educational purposes and those involving the operation of the school.
4. Computer equipment (other than staff issue laptops) should not be taken off site without formal authorisation of EBS ICT Support.
5. Software must be approved by the Head of ICT Services before purchase or installation.
6. Software licences and original media must be given to the Head of ICT Services in case proof of ownership is required. Failure to do so may result in that software being withdrawn from use.

### B. Standard Equipment

1. Please be aware that you are accountable for equipment being used by students under your supervision.
2. Do not install, or attempt to install hardware of any type on the EBS ICT network without the permission of a member of EBS ICT Support.
3. Do not connect, or attempt to connect personal mobile equipment (e.g. laptops, Tablets, Mobile Phones, PDAs etc.) to the EBS network without consulting a member of EBS ICT Support.

### C. Staff Laptops

1. Laptops and accessories issued to you remain the property of the school and are on loan whilst you are employed at the School.
2. Laptops should never be left in an unattended car or public place.
3. Laptops should be used within school at least once a month to receive software updates.
4. The school ICT system does not routinely backup data from laptops. It is your responsibility to do this.

**D. Security and Privacy**

1. When leaving a computer unattended, always use the Ctrl/Alt/Del function to lock the screen.
2. Do not attempt to bypass or alter security settings put in place on the EBS networks. They are there to protect you, your work and school resources.
3. Be aware of those around you when viewing confidential or sensitive information. Do not access sensitive information in public places like internet cafes or coffee bars.
4. Any printed 'hard copy' of confidential or sensitive information must be kept securely and shredded when finished with.
5. Do not trespass in other people's folders, work or files.

**E. Internet**

1. Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
2. You are expected to exercise professional conduct when accessing the web - visiting only sites appropriate for viewing in a school environment.
3. Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.

**F. Email**

1. Take care opening attachments or clicking on links in an email. These can contain viruses or other programmes that could cause extensive damage to the EBS ICT systems. If in doubt, consult EBS ICT Support.
2. The use of strong language, swearing or aggressive behaviour will not be permitted.
3. Emails containing material with violent, dangerous, racist, or inappropriate content must be reported to a relevant member of staff. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden.

**I have read this document and the e-safety policy carefully. I understand that serious breaches of these policies may result in disciplinary action.**

Staff Name: _____

Staff Signature: _____ Date: _____

Username: _____

Email: _____@eastbarnetschool.com