Bardfield Academy

E-Safety Policy

Reviewed 2016

E-Safety Policy

The Internet is part of everyday life for education, business and social interaction and schools have a duty to provide students with quality Internet access as part of their learning experience. Pupils use the Internet outside school and need to learn how to evaluate Internet information and to take care of their own safety and security. Internet use has been shown to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management function.

The school's Internet access has been designed to enhance and extend education and pupils will be taught what Internet use is acceptable and what is not.

As part of our home school agreement, parents are asked for permission for their child to access the Internet. Pupils are not allowed to access the Internet without adult supervision. Under the computing curriculum, pupils use the Internet for research and they will be taught to be critically aware of the materials they read and how to validate information before accepting its accuracy.

Network Security

DUCL supply schools in the South East with their broadband connection through the Local Authority. This is filtered for inappropriate content using the Protex system, which has been independently tested and approved for school use. There are two main servers in use in the school and both are located in secure areas with physical access restricted.

- The whole network is covered by up to date anti-virus protection.
- Wireless devices are proactively managed and secured with WPA2 encryption.
- The security of the school's information systems and users will be reviewed regularly.
- Personal data sent over the internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by an anti-virus/malware scan.
- Unapproved software will not be allowed in work areas or attached to emails.
- Files held on the school's network will be regularly checked.
- The ICT management team will review system capacity regularly.
- The use of user logins and passwords to access the network will be enforced.

Levels of Internet access and supervision will vary according to the pupil's age and experience. Teachers may need to research areas including drugs, bullying, racism or harassment. In such cases, legitimate use is recognised and profile restrictions removed temporarily. A 'walled garden/allow list' restricts access to a list of approved sites. Such lists inevitably limit pupil's access to a narrow range of content. The Protex system filters out inappropriate content. However, it is important to recognise that filtering is not 100% effective. Occasionally mistakes may happen and inappropriate content may be accessed which is why pupils' internet use is supervised. If pupils or staff discover unsuitable sites, they should turn their screens off and report the incident to the E-Safety Officer/ICT management team, who will escalate the concern as appropriate. An incident log is in place to report breaches of filtering or inappropriate content being accessed.

Emails

Staff will only use official school provided email accounts for school business. Pupils only use approved in-house email accounts for school purposes and must immediately tell a designated member of staff if they receive offensive email. A Hector's World safety button is available for children to hide anything offensive and report any such instances. Pupils are taught the dangers of revealing personal details about themselves and others. Pupils are taught that any email conversations are carried out in a manner comparable to speaking to a person face-to-face, with

manners, courtesy, respect and common sense. Contents of emails are subject to the Data Protection Act and the Computer Misuse Act.

Website

The Headteacher takes overall responsibility for the online content published by Bardfield Academy and will ensure that it is accurate and appropriate.

No staff personal details will be published. Images or videos that include pupils will be carefully selected; pupils full names will not be used anywhere on the website, particularly in association with photographs. Permission is obtained from parents/carers for images/videos to be electronically published as part of the Admission process. Pupil's work will only be published with their permission or their parents. Written consent will be kept by the school where pupil's images are used for publicity purposes until the image is no longer in use.

Images

Photographs and videos can be effective ways to show parents and the local community the activities and learning that takes place within the school.

The taking of photographs and videos of pupils purely for personal reasons, such as by parents at Sports Day or grandparents videoing a play, is not a breach of the Data Protection Act. However, any such photographs/videos are for personal use and cannot be sold or put on the web/internet, as that would convene Data Protection legislation. The school will inform parents of any events where parents may take digital images and give them the chance to advise if they do not want their child to be photographed/filmed.

If pupils take part in public performances or other activities outside the school premises where digital images will be taken, permission will be sought from parents/carers for these to be taken and used publically.

If the school suspects a person of taking unauthorised photographs or undertaking unauthorised filming of children, the appropriate authority will be contacted immediately.

Mobile phones – virtually all mobile phones now contain a facility to take photographs and videos. The same rules apply to images taken on phones as any other devices. When pupils bring mobile phones into school, these should be given to their class teacher and stored in a secure place until the end of the day. Pupils are not to use mobile phones to take photographs/videos of any members of staff or pupils.

All images taken by the school will be stored on password protected devices. Images of pupils are not to be taken off the premises unless permission is granted on a case by case basis by either the Headteacher or the Senior Leadership Team. Photographs of children that leave the school will not be used for more than a year after they have left unless parental consent has been obtained for their photographs to be used for official publications e.g. the school brochure.

Appendix 1 – School Admission form containing consent for use of images of children.

Appendix 2 – Guidance for Parents/Carers using photography/video at an event.

Appendix 3 – Staff, Governor and Visitor Acceptable Use Agreement

Mobile Devices

If pupils bring mobile devices (including mobile phones) into school, they are to be given in at the office to store until the end of the day. The school accepts no responsibility for the loss, theft or damage of any mobile devices, nor will the school accept responsibility for any adverse health effects caused by any such devices, either potential or actual.

No mobile devices are permitted to be used in certain areas within the school site, such as changing areas, toilets and the swimming pool area, by any member of the school community.

If a pupil breaches the school policy then the device will be confiscated and held in a secure place until the end of the school day in accordance with the school policy.

Staff are not permitted to use their own personal devices for contacting children or their families within or outside the setting in a professional capacity and will have access to a school phone where contact is required. Mobile devices are to be switched off or put on silent mode and Bluetooth communication should be 'hidden' or switched off. Mobile devices will not be used during teaching periods unless permission has been given by a member of the Senior Leadership Team in emergency circumstances. Use of a mobile device during break/lunch periods should not be in places where children are present – in the playground or corridors for example.

Staff should not use mobile devices to take images of children and only school provided equipment is to be used.

Social Networking, Social Media and Personal Publishing

The internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

For responsible adults, social networking sites provide easy to use free facilities, although advertising often intrudes. Pupils are encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

Examples of social media and personal publishing tools include blogs, wikis, social networking, forums, bulletin boards, multi-player online gaming, chatrooms, instant messaging and many others.

In order to protect the school and individuals within the organisation, members of staff are not allowed to discuss, comment or mention the school directly or indirectly on any social networking sites where these are being used personally (i.e. they are not school sites involved in promoting the school) unless clear authorisation is given.

Under no circumstances:

- Must comments be made that are derogatory to the school or any member of staff or individual within the school.
- Must confidential information be posted or discussed on any sites
- Must any information relating to the school's affairs be posted on sites – this may include operational matters, restructures, changes in personnel etc.
- Should members of staff run social network spaces for pupils to use on a personal basis.

Personal publishing/blogging etc. will be taught via age appropriate sites that are suitable for educational purposes where they are moderated by the class teacher or ICT management team.

Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Concerns regarding pupils' use of social networking, social media and personal publishing sites (in and out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.

Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction. Safe and professional behaviour will be outlined in the school's Acceptable Use Agreement. (*Appendix 3)* Visitors to the site, who require access to the school's network or Internet access, will also be asked to read and sign a copy of this agreement.

As part of the Admissions process, parents/carers are asked to sign an Acceptable Use Agreement for pupils. Parents are required to discuss the agreement with their child and sign a copy which will be kept in their personal folders. *(Appendix 4)*

No members of the school community should publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

Emerging technologies will be examined for educational benefit and a risk assessment undertaken.

Cyber-bullying

Cyber-bullying, along with all other forms of bullying, of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

There are clear procedures in place to support anyone in the school community affected by cyber-bullying. Pupils, staff and parents/carers are advised to keep a record of the bullying as evidence; the school will take steps to identify the bully where possible and appropriate. Pupils, staff and parents/carers are required to work with the school to support our approach to cyber-bullying and the school's E-Safety ethos.

Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and in line with our Data Protection Policy.

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer/laptop. Neither the school, nor the South Essex Academy Trust, can accept liability for the material accessed, or any consequences resulting from Internet use.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the police. Methods to identify, assess and minimise risks will be reviewed regularly.

When considering access for vulnerable members of the school community (such as children with special educational needs) the school will make decisions based on the specific needs and understanding of the pupils(s).

E-safety training is carried out across the school using age appropriate material and is revisited at least once a year for all pupils, with e-safety rules being posted in every classroom. Safe and responsible use of the internet and technology will be reinforced across the curriculum and subject areas.

Up-to-date and appropriate staff training in safe and responsible internet use, both professionally and personally, will be provided for all members of staff.

A partnership approach to e-safety at home and school with parents is encouraged. Information and guidance to parents/carers on e-safety will be made available in a variety of formats, including useful links available on our website.

Dealing with incidents

All members of the school community will be informed about the procedure for reporting e-safety concerns (such as breaches of filtering, cyber-bullying, illegal content etc.) The E-Safety Officer will record all reported incidents and actions taken in the school's e-safety incident log and any other relevant areas e.g. Bullying or Child Protection log.

The designated Child Protection Officer will be informed of any e-safety incidents involving Child Protection concerns, which will then be escalated appropriately.

Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures. Any complaints about Internet misuse will be dealt with under the school's complaints procedure. Parents and pupils are asked to work in partnership with the school to resolve issues.

A flow chart detailing the school's approach to e-safety incidents is attached to this policy *(Appendix 5).*

……Pink Admissions Form here…..

Guidance for Parents/Carers wishing to use photography/video at a school event.

Generally, photographs and videos for schools and family use are a source of innocent pleasure and pride, which can enhance self-esteem for children and their families. By following some simple guidelines we can use such materials safely and with regard to the law.

1. The Headteacher and the Trust Directors have the responsibility to decide if photography and videoing of organisation performances or events is permitted.
2. Parents, carers and their families can use photographs and videos taken at our school events for their own personal use only. Such photographs and videos cannot be sold and must not be put on the web/internet as that would contravene Data Protection legislation.
3. Recording and/or photographing other than for private use would require the consent of all the other parents whose children may be included in the images.
4. Parents and carers must follow guidance from staff as to when photography and videoing is permitted and where to stand in order to minimise disruption to the activity. Restrictions on photograph also apply to video and camera phones.
5. We ask you to turn mobile and camera phones to 'silent' during performances or events to prevent disruption to others.
6. Parents and carers must not photograph or video children changing for performances or events or in areas not designated by the school as being acceptable.
7. If you are accompanied by people that school staff do not recognise, they may need to check out who they are if they are using a camera or video recorder.

Staff and Visitor
ICT Acceptable Use Agreement

ICT (including data) and the related technologies such as e-mail, 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 Headteacher or Senior Management.

- I will only use the school's email, Internet, Intranet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or the Trust Directors.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, personal e-mail address and social networking identities to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on Scholarpack software) 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 Headteacher or the Trust Directors. Personal or sensitive data taken off site must be encrypted using the encrypted memory stick provided.
- I will not install any hardware of software without permission of the ICT team.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with the consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- 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.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

This Acceptable Use Agreement is a summary of our E-Safety Policy which is available in full on request.

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …… Date ……

Full Name ……(Please print)

Job title . . . . . .

Pupil ICT Acceptable Use Agreement

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address when e-mailing through the a school based email system.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my network login or any other passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will use the Hector's World button and tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my e-Safety.
- I understand that my teacher can monitor everything I do, or view on the Internet.
- I promise to turn my monitor off, or use the Hector's World button, if I see anything that upsets me and report it to an adult.

Pupil ICT Acceptable Use Agreement

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies, etc. has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these e-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the school office.

This Acceptable Use Agreement is a summary of our e-Safety Policy, a copy of which is available from the school office or can be found on the school website at bardfieldacademy.org.

✂----------

Parent/ carer signature

We have discussed the school's ICT Acceptable Use Agreement with our child and

…… (Child's name) agrees to follow the E-Safety

rules and to support the safe use of ICT at Bardfield Academy.

Parent/ Carer Signature ……

Class …… **Date** **……**

E-Safety Procedure

Appendix 5

E-Safety Incident Occurs