

Sandringham Campus
 Sandringham Road
 Barking, Essex IG11 9AG

Tel: 020 3967 7030
Fax: 020 8270 4090

www.barkingabbeyschool.co.uk
 Headteacher: Jo Tupman



BARKING ABBEY SCHOOL
 Give and expect the best

Longbridge Campus
 Longbridge Road
 Barking, Essex IG11 8UF



office@barkingabbeyschool.co.uk
 6thform@barkingabbeyschool.co.uk

E-Safety Policy

Policy Adoption

Date	Reviewed/Adopted by	Next review date	Review Frequency
13/02/2019	Resources Committee	February 2019	Annually

Governing Body Approval

Signed	Title
	Chair of Governors
	Headteacher

Document Control

Date	Version	Author	Notes
01/02/2016	1.00	A Falzon	Updated Policy
03/02/2019	1.10	P Leake	Amended format Amended section 3.4 to clarify procedures

Contents

E-Safety Policy	1
Policy Adoption.....	1
Governing Body Approval	1
Document Control	1
Introduction	3
1 Policy Statement.....	3
2 Teaching and Learning.....	3
2.1 Why is Internet and digital communication use important?	3
2.2 How does the Internet benefit education?.....	3
2.3 How will Internet use enhance learning?.....	3
2.4 How will students learn to evaluate Internet content?	3
2.5 How will e-mail be managed?	4
2.6 How will Web site content be managed?	4
3 Internet use and social networking	4
3.1 What are newsgroups and e-mail lists?	4
3.2 Can Chat be made safe?.....	5
3.3 How can emerging Internet applications be managed?	5
3.4 How will Internet access be authorised?	5
3.5 How will the risks be assessed?	5
3.6 How will filtering be managed?	5
3.7 Video Conferencing.....	6
3.8 How will the policy be introduced to students?	6
3.9 How will staff be consulted?	6
3.10 How will ICT system security be maintained?.....	6
3.11 How will complaints regarding Internet use be handled?	7
3.12 How will parents' support be enlisted?	7
3.13 How is Internet used across the community?.....	7
3.14 How will digital media be used safely?	7

Introduction

This Policy relates to other policies including those for ICT, Child Protection, Safe Practice Policies, behaviour including Anti Bullying Policy and for PSHE and citizenship. Staff, parents, governors and students have been consulted in deciding the policy.

Our Internet Policy has been written by the school, building on the Barking and Dagenham as well as government guidance. It has been agreed by the senior management and approved by governors. It will be reviewed annually.

1 Policy Statement

- If printed, copied or otherwise transferred from this website this document must be considered to be an uncontrolled copy.
- Policy amendments may occur at any time and you should consult the Policies page on the website for the latest update.

2 Teaching and Learning

2.1 Why is Internet and digital communication use important?

- The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with high-quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary learning tool for staff and students.

2.2 How does the Internet benefit education?

- Access to world-wide educational resources including museums and art galleries;
- inclusion in government initiatives such as the DfES ICT in Schools
- educational and cultural exchanges between students world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for students and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues; improved access to technical support including remote management of networks;
- Exchange of curriculum and administration data with the LA and DfES.

2.3 How will Internet use enhance learning?

- The school Internet access will be designed expressly for student use and will include filtering appropriate to the age of students.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of students.
- Staff will guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity.
- Students at Key Stage Three and Four will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2.4 How will students learn to evaluate Internet content?

- If staff or students discover unsuitable sites, the URL (address) and content must be reported to the E-Safety Coordinator in the first instance

- Schools will ensure that the use of Internet derived materials by staff and by students complies with copyright law.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

2.5 How will e-mail be managed?

- Students may only use approved e-mail accounts on the school system and the forwarding of chain mail letters is not permitted.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone without specific permission.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and will be restricted.
- E-mail sent to an external organisation will be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Incoming e-mail will be treated as suspicious and attachments not opened unless the author is known.

2.6 How will Web site content be managed?

- The point of contact on the Web site will be the school address, school e-mail and telephone number. Staff or students' home information will not be published.
- Web site photographs that include students will be selected carefully and will not enable individual students to be clearly identified.
- Students' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school Web site.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Web site will comply with the school's guidelines for publications.
- The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained. E.g. the use of Internet derived materials by staff and by students complies with copyright law.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
(Children, Families, Health and Education Directorate page 6 June 2008)

3 Internet use and social networking

3.1 What are newsgroups and e-mail lists?

- Newsgroups will not be made available to students unless an educational requirement for their use has been demonstrated.
- If this is demonstrated, the school will control access to social networking sites, and consider how to educate students in their safe use.
- Students will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Students will not place personal photos on any social network space without considering how the photo could be used now or in the future.
- Students will be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students will only invite known friends and deny access to others.

3.2 Can Chat be made safe?

- Students will not be allowed access to public or unregulated chat rooms.
- Children will use only regulated educational chat environments. This use will be supervised, and the importance of chat room safety emphasised.
- A risk assessment will be carried out before students are allowed to use a new technology in school.

3.3 How can emerging Internet applications be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- As a school we understand that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- The use by students of cameras in mobile phones will be kept under review.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.
- Staff will school a school phone where contact with students is required.
- As a school, we will liaise with parents on emerging applications available at home such as FACEBOOK. Their benefits and possible consequences of misuse will be highlighted.

3.4 How will Internet access be authorised?

- The school requires parents/students to sign an agreement before allowing internet access. This confirms they have read and agreed to core school policies including ICT Acceptable Use Policies.
- Students at KS3 and KS4 will be provided with supervised Internet access.
- In addition to signing the acceptable use document students (and staff) have an online agreement that they have to agree to every 90 days. Declining this will result in the individual being logged off.

3.5 How will the risks be assessed?

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for students. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Headteacher will ensure that the E-Safety policy is implemented and compliance with the policy monitored.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

3.6 How will filtering be managed?

- The school will work in partnership with parents, the LA, DfES and the Internet Service Provider to ensure systems to protect students are reviewed and improved.
- If staff or students discover unsuitable sites, the URL (address) and content must be reported the E-Safety co-ordinator.
- The network manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Filtering strategies will be selected by the school, in discussion with Barking and Dagenham LA. The filtering strategy will be selected to suit the age and curriculum requirements of the student.

3.7 Video Conferencing

- Video conferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
- Students will ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the Students' age.

3.8 How will the policy be introduced to students?

- Rules for Internet access will be posted in all rooms where computers are used.
- Students will be informed that Internet use will be monitored.
- Instruction in responsible and safe use will precede Internet access.
- Students will be reminded of the rules and risks at the beginning of any lesson using the Internet
- A module on responsible Internet use will be included in the PDC programme, ICT lessons and other appropriate subject areas, covering both school and home use.
- E-Safety rules will be reinforced regularly as opportunities present themselves during Assemblies, parent link evenings, lessons etc.
- Students will be informed that network and Internet use will be monitored.
- An ongoing programme of training in e-Safety will take place within the school to keep abreast of new risks and threats.

3.9 How will staff be consulted?

- All staff are governed by the terms of the 'Responsible Internet Use' in school.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and its importance explained.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures will be supervised by senior management.
- Staff development in safe and responsible Internet use and on the school Internet policy will be provided as required.
- All staff will be given the School e-Safety Policy and its importance explained.
- Staff will understand that phone or online communications with students can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.

3.10 How will ICT system security be maintained?

- The school ICT systems are reviewed regularly with regard to security.
- Virus protection is installed and updated regularly.
- Security strategies are discussed with the LA, particularly where a wide area network connection is being planned.
- Personal data sent over the Internet will be encrypted or otherwise secured however the school cannot be held responsible for the use of secure pass worded sites from within school. The school's security measures may not prevent losses due to key logging or data theft when people access on line banking/emails etc on the school system.
- Unapproved system utilities and executable files will not be allowed in students' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- The network manager will ensure that the system has the capacity to take increased traffic caused by Internet use.

3.11 How will complaints regarding Internet use be handled?

The school has agreed a course of action for handling e-safety incidents. The Pastoral Co-ordinator will most likely come into contact with any e-safety issue first. Pastoral Co-ordinator to then liaise with:

- 1 Network Manager if its on 'Acceptable use policy abuse'
 - 2 Child Protection Officer if it's a 'child protection issue'
 - 3 School Police Officer if it's a Police/Criminal matter
 - 4 Assistant Headteacher (Mr Falzon) to also be informed in all cases.
 - 5 Any complaint about staff misuse must be referred to the Headteacher.
- Students and parents will be informed of the complaints procedure.
 - Parents and students will need to work in partnership with staff to resolve issues.
 - As with drugs issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
 - Sanctions available include:
 - interview/counselling;
 - informing parents or carers;
 - Removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system, including examination coursework.

3.12 How will parents' support be enlisted?

- Parents' attention will be drawn to the School Internet Policy in newsletters, the school brochure and on the school Web site and 'parent link Evening workshops'.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations such as Child Exploitation and Online Protection (CEOP).
- The school will maintain a list of e-safety resources for parents/carers.

3.13 How is Internet used across the community?

- Adult users will need to sign the acceptable use policy.
- Parents/carers of children under 16 years of age will generally be required to sign an acceptable use policy on behalf of the child.
- The school will liaise with local organisations to establish a common approach to e-safety.

3.14 How will digital media be used safely?

- The school has produced a checklist for teachers to adhere to. This can be summarised as follows:
- A student's name must never be linked to a photograph or moving image. E.g. pictures of sporting events or sports teams winning events sent to newspapers for printing. As a school we also wish to celebrate success by displaying photographs of students. Due to the openness of the school; we have various visitors during the day, open evenings and public functions etc, student names must never be associated with the pictures. Parents/guardians are aware of this and sign a 'photograph-audio disclaimer'.
- To this end, the school' 'photograph-audio disclaimer' must be adhered to at all times.
- Tapes that are reused must always be 'blanked' first.
- Unused DVDs with content on must always be shredded.
- Guardians permission must always be sought after when videos are being outsourced, e.g. for publicity etc.
- Students will always be consulted on the final DVD produced.
- Certain videos will be water marked so that images cannot be misused.
- Master copies of videos will be kept in a secure area monitored by CCTV.

- Student images on Barking Abbey's school MIS system can only be accessed by teachers using a username and password (teachers understand not to display this information on the visualiser; passwords are also changed regularly).
- Online video uploaded to Vimeo have had the Comment section disabled, to prevent any bullying comments being left, and also download of the video file is disabled.
- When videos are made for school departments, the above guidelines are made clear and any areas of uncertainty will be discussed with the E-Safety officer first.