



NORTH BIRMINGHAM ACADEMY

E-Safety Policy

Writing and reviewing the E-safety policy

The E-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, Anti Bullying and for Safeguarding.

The school's ICT Service Delivery Manager along with the Head Teacher will also act as the schools E-Safety Coordinator.

Our E-Safety Policy has been written building on the BGFL E-Safety Policy and government guidance and Safeguarding procedures. It has been agreed by senior management and approved by governors. The E-Safety Policy and its implementation will be reviewed annually.

Teaching and Learning

Why Internet use is important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and Students.

Internet use will enhance learning

The school Internet access is designed expressly for pupil use and includes 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. Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Students will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and Students complies with copyright law. Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information System Security

School ICT systems capacity and security will be reviewed regularly.

Virus protection is updated regularly.

Advice on security strategies will be monitored on the School's ICT web page and clarification sought as necessary.

E-mail

Students may only use approved e-mail accounts on the school system and email usage will be supervised and monitored by a staff member.

Students must immediately inform a teacher if they receive offensive e-mail.

Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

The forwarding of chain letters is not permitted.

Please note: Access to external email accounts such as Hotmail & Yahoo will not be permitted.

Published content and the school web site

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or Students' personal information will not be published.

The ICT Service Delivery Team will take overall editorial responsibility and ensure that content is accurate and appropriate. **Publishing pupil's images and work**

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.

Pupil's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

The school will block/filter access to social networking sites such as Facebook and MSN Messenger etc.

Newsgroups will be blocked unless a specific use is approved. Students will be advised never to give out personal details of any kind that may identify them or their location.

Students and parents will be advised that the use of social network spaces outside school is inappropriate for Students.

Managing filtering

The school will work with the LA, DCSF and the Internet Service Provider to ensure systems to protect Students are reviewed and improved.

If Staff or Students discover an unsuitable site, it must be reported to the E-Safety Coordinator.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

When this becomes available within the school, videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.

Students will be required to gain permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing will be appropriately supervised for the Students' age.

Managing emerging technologies

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.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

Authorising Internet access

All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.

The school will keep a record of all staff and Students who are granted Internet access. The record will be kept up-to-date, for instance, a member of staff may leave or a Student's access be withdrawn.

Parents will be asked to sign and return a consent form.

Assessing risks

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 Local Authority (LA) can accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the head teacher.

Complaints of a Child Protection nature must be dealt with in accordance with school child protection procedures.

Students and parents will be informed of the complaints procedure.

Discussions will be held with the the schools Safer Schools Partnership Police Officer to establish procedures for handling potentially illegal issues

Communications Policy

Introducing the e-safety policy to Students

E-safety rules will be posted in all networked rooms and discussed with the Students at the start of each year.

Students will be informed that network and Internet use will be monitored through Policy Central.

Staff and the e-Safety policy

All staff will be given the School e-Safety Policy and its importance explained.

Staff should be aware that Internet traffic is monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

Approved by NBA Governors

Date of Next Review:

Lead Manager: