

Bradford Grammar Junior School

E-Safety

Policy Document

Bradford Grammar Junior School E-Safety Policy

Contents

E-Safety Policy Introduction and Definitions	3
Roles and Responsibilities	4
Whole School e-safety	4
Teaching and learning	4
Internet use that will enhance learning	5
Managing Internet Access.....	5
E-mail.....	6
Published content and the school website	6
Social networking and personal publishing	7
Managing filtering.....	7
Managing video-conferencing	7
Managing emerging technologies	8
Protecting personal data	8
Handling e-safety complaints	8
Communications Policy	9
Staff and the e-Safety policy	9
Enlisting parents' support.....	9
Activities: Key e-safety issues - Relevant websites.....	9

E-Safety Policy Introduction and Definitions

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging (<http://www.msn.com>, <http://info.aol.co.uk/aim/>) often using simple web cams
- Blogs / Twitter etc. (and other on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular www.myspace.com / www.piczo.com / www.bebo.com / <http://www.hi5.com>)
- Video broadcasting sites (Popular: <http://www.youtube.com/>)
- Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)
- Gaming Sites (Popular www.neopets.com, <http://www.miniclip.com/games/en/>, <http://www.runescape.com/>)
- Music download sites (Popular <http://www.apple.com/itunes/> <http://www.napster.co.uk/> [http://www-kazaa.com/](http://www.kazaa.com/), <http://www-livewire.com/>)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

E-Safety highlights the need to educate pupils about the benefits and risks of using this technology and provides safeguards and awareness for users to enable them to control their online experience.

This policy establishes the ground rules we have for using the Internet, electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experiences. It also describes how these ideas fit in to the wider context of discipline and PSHCE policies and demonstrates the methods used to protect children from sites containing pornography, racist or politically extreme views and violence.

The previous Internet Policy has been revised and is now specific to the Junior School and renamed as the Schools' e-Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole. Staff should also make themselves aware of the whole school approach to ICT contained within the whole school Staff Handbook.

The e-Safety Policy is part of the School Development Plan.

The school's e-safety policy should operate in conjunction with other policies including:

Child Protection (see whole school Staff Handbook) Pastoral care, Anti-Bullying, Curriculum, Data protection (see whole school Staff Handbook) and the school ICT Curriculum document.

Roles and Responsibilities

Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The Headmaster ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to the ICT coordinator.

Our school **e-Safety Co-ordinator** is Chris Newsome.

The **Designated Child Protection Officer** is: Neil Gabriel (Junior School – Michael Sharp Senior School).

Our e-Safety Coordinator ensures the school keeps up-to-date with e-Safety issues and guidance through organisations such as Becta and The Child Exploitation and Online Protection (CEOP).

The Policy is available for staff in the ICT live folder in the school shared area and for parents upon request.

Whole School e-safety

E-Safety depends on effective practice at a number of levels:

Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.

Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.

Safe and secure broadband, including the effective management of filtering (see the whole school ICT policy on filtering).

The overriding rule is that no pupil should have *any* unsupervised access to the computers within school.

Teaching and learning

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 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 pupils.

Internet use that will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering. No site should be visited by pupils unless the teacher in charge has first visited the site and checked out links etc. This is vital as the filtering relates to the whole school and, as such, access to some sites may be acceptable for six form pupils but unsuitable for the Junior School. Obviously extreme sites are filtered, as are gaming sites but occasionally as with all systems things can creep through.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. This is laid out in the ICT scheme document.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Teachers will ensure that the use of Internet derived information, for research and projects, complies with copyright law. Pupils should be made aware that the Internet is not a free for all and that much of its content is covered by copyright law.
- Pupils should be taught to be critically aware of any Internet derived material they read and shown how to evaluate and validate the content before accepting its accuracy.

Managing Internet Access

- School ICT systems capacity and security will be reviewed regularly.

- Staff and pupils' use of the Internet is monitored. Any unacceptable use is sent to the Head and Director of ICT and discussed with the Headmaster of the Junior School who will decide on the action to be taken.
- Virus protection and restricted sites are updated regularly. However, due to the school network being for the whole school and not specifically the Junior School, some sites that are acceptable for Senior School are not acceptable for Clock House.
- **Therefore, when using search engines to access information from a range of websites pupils must always be supervised and the search carried out by the teacher prior to the lesson to avoid any unsuitable names and sites cropping up.**

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in any e-mail communication, or arrange to meet anyone.
- 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.

In reality much of the above should not be an issue as the teacher is required to monitor e-mails and they should only be sent after they have been read. This also applies in the case of e-pals where we occasionally allow pupils to contact children in other schools abroad. The schools policy is that these emails should be composed on Microsoft Word and having been approved by the teacher pasted into an email.

Published content and the school website

- The contact details on the website should be the school address, e-mail and telephone number. Staff names and photographs are published but can be removed if requested.

- All parents are required to sign a form indicating whether or not their child's photograph may or may not be published in school magazines and on the website etc.
- The Junior School generally avoids the use of pupil names and photographs together on the website except when impossible to do so (an individual sports winner for example). All parents are asked to opt out should they not want an image of their child to appear on the web-site.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

If staff or pupils discover an unsuitable site, it must be reported to the ICT Coordinator / form teacher or Headmaster or Deputy Head as soon as possible (they will get the site blocked).

Managing video-conferencing

IP video-conferencing should only be used when pupils are with a teacher and permission of the Headmaster has been sought.

Video-conferencing will be appropriately supervised for the pupils' age.

Managing emerging technologies

- New and 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. All pupils are informed that the use of telephones in school is not allowed without the permission of a teacher. They are also informed that using a mobile phone or email to tease, bully or otherwise upset pupils, even if outside school, may be punishable within school.
- All mobile phones are handed to the form teacher at morning registration and handed back to pupils at the end of the day.

Protecting personal data

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

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff. Pupils can, as per the Anti-Bullying, Pastoral Care and other policies, approach any member of staff with a concern.
- Any complaint about staff misuse must be referred to the Headmaster.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by e-Safety Coordinator / Headteacher;
- 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 coursework];
- referral to Child Protection Officer and in extreme situations the Police.

Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.
- Each year, in each year group, a lesson on e-safety will be taught at the beginning of the autumn term.

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 can be 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 website.
- As part of the 'Every Child Matters' agenda, pupils and parents are informed of the Exploitation and Online Protection Centre: www.thinkyouknow.co.uk.

Activities: Key e-safety issues - Relevant websites

Creating web directories to provide easy access to suitable websites. At the time of writing staff are sharing resources but it is hoped that a central location will be used to store suitable websites under subjects and topics.

Safe educational websites are also posted on the school website on the Learning and Fun Page. Parents are also encouraged to pass on suitable sites for inclusion if appropriate. Other sites include:

Ask Jeeves for kids

Yahooligans

CBBC Search