Birchwood High School
e-Safety Policy

Responsibility

Internet safety depends on staff, governors, parents and the students themselves taking responsibility for the use of internet and other communication technologies such as mobile phones. The balance between educating students to take a responsible approach and the use of regulation and technical solutions will be judged carefully. The school and Hertfordshire County Council limit internet access, in line with this e-safety policy.

As e-Safety is an important aspect of strategic leadership within the school, the Principal and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety co-ordinator in this school is Melinda Mulley who has been designated this role as a member of the senior leadership team, John Burrisson is also named as the technical coordinator of e-Safety. All members of the school community have been made aware of who holds this post. It is the role of the e-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as HCC, Herts for Learning Ltd, CEOP (Child Exploitation and Online Protection) and Childnet.

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

At Birchwood High School we understand the responsibility to educate our students on e-Safety 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.

Senior Leadership and governors are updated by the e-Safety Co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements 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 behaviour/pupil discipline (including the anti-bullying) policy and PSHE.

e-Safety and the Curriculum

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 on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote e-Safety.

Educating students about the online risks that they may encounter outside school is done informally when opportunities arise, through assemblies and as part of the e-Safety curriculum

Students are taught about respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities

Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying, including peer on peer abuse. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; ie parent/carer, teacher/ trusted staff member, or an organisation such as Childline or the 'CEOP report abuse' button.

Equal Opportunities - Students with Additional Needs

The school endeavours to create a consistent message with parents/carers for all students and this in turn should aid establishment and future development of the schools' e-Safety rules.

However, staff are aware that some students may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a student has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned and well managed for these children and young people

Authorisation of Use
- The school supplies internet access to all staff and students. A record will be kept of those who have their internet usage suspended and details of any violation.

- Students must agree to the Acceptable Use Policy at every logon in order to use the school network.

Filtering
The school will work in partnership with parents, Herts for Learning and Hertfordshire County Council to ensure systems to protect students are reviewed and improved. Hertfordshire Local Authority has a monitoring solution via the Hertfordshire Grid for Learning where web-based activity is monitored and recorded. School internet access is controlled through the HICS web filtering service. For further information relating to filtering please go to http://www.thegrid.org.uk/eservices/safety/filtered.shtml

There are no straightforward or totally effective solutions and staff, parents and the students themselves must remain vigilant.

- The school internet access is designed expressly for educational use and is filtered.
- Students learn appropriate internet use.
- Access to the internet may be unsupervised eg at lunchtimes.

Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.
- Our school uses Facebook and Twitter to communicate with parents and carers. Mary Augustine is responsible for all postings on these technologies and monitors responses from others

- Staff are able to setup Social Learning Platform accounts, using their school email address, in order to be able to teach students the safe and responsible use of Social Media

- Students are not permitted to access their social media accounts whilst at school

- Staff, governors, students, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others

- Staff, governors, students, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever

- Staff, governors, students, parents and carers are aware that their online behaviour should at all times be compatible with UK law

- The use of inappropriate text, images and videos about other students or staff is unacceptable and will always be fully investigated once discovered

- 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

- 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

- 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)

- Our students are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals

- Students are encouraged to be wary about publishing specific and detailed private thoughts and information online

- Our students are asked to report any incidents of Cyberbullying to the school

Risk Assessment
- 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. The school cannot accept liability for the material accessed, or any consequences of internet access.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Evaluating Content
- The technical co-ordinator will be responsible for permitting and denying additional websites as requested by colleagues.
- Students will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

School Website Content
- The point of contact on the website should be the school address, school e-mail and telephone number.
- Website photographs that include students will be selected carefully.
- Photographs of students may only be published on the school website if parents have given permission.

E-Mail
- Students may only use their school e-mail account on the school system.
- Students must immediately report any offensive e-mails to the class teacher or form tutor.
- Students must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone through an e-mail contact.
- Students must not send multiple copies of e-mails.

Mobile Phones
- Students are allowed to bring mobile phones to school, but they must be switched off and out of sight.
- The sending of abusive or inappropriate text messages is forbidden.
- If used inappropriately, mobile phones will be confiscated.

e-Safety message to Students and Parents

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used. The e-Safety policy will be introduced to the students at the start of each school year. e-Safety posters will be prominently displayed.

- The key e-Safety advice will be promoted widely through school displays, newsletters, class activities, assemblies and is sent to all parents via letter, the school website, newsletter and parental engagement events where appropriate.

eSafety message to Staff
- All staff must refer to the relevant detail in the staff handbook and adhere to the IT Usage Staff Policy.
- Staff should be aware that internet traffic is monitored and reported by the school and can be traced to an individual computer. Discretion and professional conduct is essential.
- The monitoring of internet use is a sensitive matter. Staff that operate monitoring procedures should be supervised by senior management.
- Staff development in safe and responsible internet use and on the school internet policy will be provided as required.

Sanctions
- The school behaviour for learning policy applies to responsible ICT use.
- Responsibility for handling incidents will be delegated to a senior member of staff.

Sanctions available include:
- Interviews with senior staff.
- Informing parents or carers.
- Removal of internet or computer access for a period.
- Possible involvement of the police.
- Any complaint about staff misuse must be referred to the Headteacher.

Links to Other Policies

This policy should be read in conjunction with the Behaviour for Learning, Anti-Bullying and Social Media policies.

Consultation

The following groups were consulted during the creation of this policy:

- School Council
- SLT
- Parents
- School governors
- Hertfordshire Internet Provider