Heaton St. Barnabas' CE (VA) Primary School

Policy For e-Safety

This policy was reviewed and updated by governors in March 2014

Signed ……………………………………………..

Position : Chair of Curriculum and Pastoral Committee

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

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.

At Heaton St Barnabas C of E (VA) Primary School we understand the responsibility to educate our pupils 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.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by staff, but brought onto school premises (such as laptops, mobile phones and camera phones.)

Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-safety co-ordinator in our school is Barbara Cormican who has been designated this role as a member of the senior leadership team. There is a wider e-safety team including the headteacher and ICT technicians working in school. All members of the school community have been made aware of who hold these responsibilities. It is the role of the e-safety co-ordinator and team to keep abreast of current issues and guidance through organisations such as Local Authority, CEfM, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/ e-safety co-ordinator/team 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 pupils, 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, P.S.H.C.E.

E-safety skills development for staff

- Our staff receive regular information and training on e-safety issues in the form of staff meetings, twilights and written correspondence.
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know to report the misuse of technology by any member of the school community to the e-safety co-ordinator or the Headteacher.
- All staff are required to incorporate e-safety activities and awareness within their planning.

Managing the school e-safety messages

- 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 pupils at the start of each school year via the primary pupil acceptable use/e-safety agreement, and to new children/parents/carers when they begin school.
- E-safety rules are displayed on the startup desktop and in the ICT suite.

E-safety in 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 pupils on a regular and meaningful basis. All staff have a responsibility to ensure that e-safety is embedded within curriculum provision and we continually look for new opportunities to promote e-safety.

- Teachers plan opportunities within a range of curriculum areas to teach about e-safety on a termly basis (minimum).
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the e-safety curriculum.
- Pupils are aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models and discussions.

Managing the Internet

Use of the Internet to Enhance Learning:

- The school internet access is designed for pupil use and includes filtering.
- Pupils are taught what internet use is acceptable and what is not.
- Internet access will be planned to enrich and extend learning activities.
- Staff will preview any recommended sites before use.
- Staff will guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of information location, retrieval and evaluation.

Authorised Internet Access

- The school maintains a current record of all staff and pupils who are granted Internet access.

- All staff must read and sign the ‘Acceptable Use Agreement’ before using any school ICT resource.
- Parents/carers are asked to sign and return a consent form for pupil access.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be recorded on the incident log, and reported to the Local Authority helpdesk via the Headteacher or e-safety co-ordinator.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- It is the responsibility of the school, by delegation to the lead ICT technician, to ensure that Anti-virus protection and filters are installed and kept up to date on all school machines.

Social Networking

The use of public social networking sites (e.g. bebo, myspace, face book) is not allowed in school.

- School will block/filter access to social networking sites and newsgroups 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 are taught not to place personal photos on any social network space.
- Staff are advised as to safe usage of sites such as facebook – e.g. strong privacy settings

Mobile technologies

- The school allows staff to bring in personal mobile phones and devices for their own use***. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device.***
- Staff are not permitted to use mobile phones / texts during lesson time.
- Currently pupils are not allowed to bring personal mobile devices/phones to school.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good ‘netiquette’. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving emails.

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents/carers or conduct any school business using personal email addresses.
- 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 email communication, or arrange to meet anyone without specific permission.
- Access in school to external personal e-mail accounts may be blocked.

Safe Use of Images

- School keeps a list of those parents/carers who have responded to say they ***do not*** permit their child/ren to have their photograph taken for use in school/council publicity or newspaper articles. (The letter states that if the slip is not returned school will assume that parents/carers/carers are happy for photographs to be taken and to appear in publications)
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips.
- Pupils are permitted to use personal digital equipment/cameras, (not mobile phones) to record images of others when on trips. However, parents will sign their agreement that these are for own use only and no such photographs will be posted on the internet under any circumstance. (This will be incorporated into the form that parents sign to give consent for trips).

Consent of adults who work at the school

- Permission to use images of all staff who work at the school is sought on induction.

Publishing pupil’s images and work

On a child’s entry to the school, all parents/carers will be asked to give permission to use their child's photographs in the following ways (those who do not consent will be listed, as above):

- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).
- This parental response is considered valid for the entire period that the child attends this school. Parents/carers may withdraw permission, in writing, at any time.

Published content and the school website and learning platform.

- Permission from parents/carers regarding photographs of their child on the school website will be sought when the child enters school (those who do not consent will be listed, as above):
- Photographs that include pupils will be selected carefully and will not include those whose parents/carers have declined permission for their inclusion.
- Pupils’ full names will not be used anywhere on the Website or Blog, especially in association with photographs.

Webcams

- Some webcam sites may contain, or have links to, inappropriate or adult material. Teachers view any webcam sites or listings before allowing pupils to do so.
- Pupils are alerted to the danger of using web cams as an extension of a chat room. Pupils need to know the risks involved when using web cams at home and at school.
- Parental consent for pupil access to suitable webcams is included in general internet consent.

Filtering

The school will work in partnership with the Local Authority and the Internet Service Provider to ensure filtering systems are as effective as possible.

The school uses a forensic monitoring service to monitor all internet use involving school equipment both within and outside school.

Managing Emerging Technologies

Emerging technologies and software will be examined by the school's leadership team. ICT leader and ICT technical support provider for educational benefit and a risk assessment will be carried out before use in school is allowed.

Information System Security

School ICT systems capacity and security will be reviewed regularly.
Virus protection will be installed and updated regularly.
School will consider advice on security strategies e.g. the Local Authority.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
The security of school mobile devices, including lap-tops, is the responsibility of the person to whom this has been allocated. School staff laptops which are likely to contain any identifiable personal data are encrypted to prevent access to personal data through loss or theft.

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.
- 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. This will be undertaken by the e-safety team, and will be in the form of an annual review/audit of the incident log. It will also include a review of any new technologies which might need to prompt policy amendment.

Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents/carers for all pupils and this in turn should aid establishment and future development of the schools' e-safety rules.
However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.
Where a pupil 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.

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting e-safety both in and outside of school.

- Parents/carers and pupils are actively encouraged to contribute to adjustments or reviews of the school e-safety policy via e-safety training, governor meetings, parents/carers questionnaire
- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child.

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)

Handling E-safety Complaints

- Complaints of Internet misuse will be dealt with by the leadership team and recorded in the Incident Log. (Appendices).
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be reported to the Named Person for Child Protection.

Pupils and parents/carers will be informed of the complaints procedure.
Pupils are encouraged to inform their teacher or other adults in school regarding anything which makes them feel uncomfortable while using ICT.

Communication of Policy

Pupils

- Rules for Internet access will be visible on desktop at startup and in ICT suite.
- Pupils will be informed that Internet use will be monitored.

Staff

- 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 are essential.

Parents/carers

- Parents/carers' attention will be drawn to the School e-safety Policy in newsletters, the school prospectus and on the school website.

Links to Other Policies

Health and Safety Policy.
Child Protection and Safeguarding Policy.
Acceptable Use Policy.
Anti-Bullying Policy.
P.S.H.C.E.

Reviewing this Policy - Review Procedure

Staff are encouraged to discuss any issue of e-safety that concerns them. Concerns should be taken to a member of the leadership team as soon as they arise.
This policy will be reviewed annually along with all safeguarding policies
The policy will be amended, where appropriate if new technologies are adopted, if the incident log audit reveals a weakness, or if Central Government change the orders or guidance in any way.

Primary Pupil Acceptable Use
Agreement / e-safety Rules

- ✓ I will only use ICT in school for school purposes.
- ✓ I will only use my own school email address when emailing.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will not tell other people my ICT 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 tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- ✓ 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 will be contacted if a member of school staff is concerned about my e-safety.
- ✓ If I use a webcam it will only be under the strict supervision of an adult, who will have checked and authorised the access (e.g. a link with a school in another country). I will follow instructions carefully.

Incident Log Year……………….

Heaton St Barnabas C of E Primary School e-safety Log

Details of ALL e-safety incidents to be brought to the attention of the e-safety Coordinator and recorded in this log. This incident log will be monitored termly by the Headteacher and any incidents referred to anonymously in HT report to Governors. Any incidents involving cyberbullying should be recorded on the 'Integrated Bullying and racist Incident Record Form 2'

Date & Time	Name of Pupil or Staff Member	Male or Female	Room and computer/ device number	Details of Incident (including evidence)	Actions and reasons

Heaton St. Barnabas' C.E. Primary School

Rossefield Road, Heaton
Bradford, BD9 4DA
Tel: 01274 545019 Fax: 01274 553910
Headteacher: Mrs Gillian Evans M.A.

Dear parent/guardian,

ICT, including the internet, email 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. On the back of this letter you will find a list of e-safety rules, forming an acceptable use agreement for your child.

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 queries or require further information,
please contact your child's class teacher. Please be aware that without this consent your child will not be able to access ICT equipment within school.

Yours sincerely

B.Cormican
Deputy Headteacher

✂---

Name of Child ____ Class __________________________

The e-safety rules have been discussed and ……………………………………………………………….. (child name) agrees to follow the rules and to support the safe use of ICT at Heaton St Barnabas C of E Primary School.

Parent/ Guardian Signature ………………………………………………………………………………………………….

Date ……

Permission to use images of Staff for school purposes:

(Permission to use images of all staff who work at the school is sought on induction.)

Name:..Position:…………………………………………

I give permission for my photograph/image to be used for identification documents, documents within school, council and newspaper publicity, our school website and documents sent to other schools, e.g Comenius project.

Signed: ....   Date: ....