Barnby Dun Primary Academy E-safety Policy

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
- 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 Barnby Dun Primary, 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, tablets, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

The Policy is part of the school's Strategic Development Plan and related to other policies including Positive Learning, Safeguarding and Data Protection policies. As legislation is often amended and new regulations introduced the references made in this policy may be superseded. For an up to date list of legislation applying to schools please refer to the Department for Education website at www.education.gov.uk/schools.

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 eSafety co-ordinator in our school is Carly May, who has been designated this role. All

members of the school community have been made aware of who holds this post. It is the role of the e-Safety coordinator to keep abreast of current issues and guidance through organisations such as Doncaster LA, Becta, CEOP (Child Exploitation and Online Protection) NSPCC and Childnet. Senior Management and Governors are updated by the Head/ eSafety coordinator 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 (appendices), 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 (including the anti-bullying) and PHSE policies.

E-Safety skills development for staff

- Our staff receive regular information and training on e-Safety issues through the coordinator at staff meetings.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see attached flowchart.)
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff are encouraged to incorporate e-Safety activities and awareness within their lessons.

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.
- E-safety posters will be prominently displayed.
- E-safety information is available on the school website.
- We will participate in the annual National Internet Safety day.

E-Safety in the Curriculum

- The school provides opportunities within a range of curriculum areas to teach about e-Safety.
- 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 taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also 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.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.
- The school will send out relevant e-safety information for parents/carers through newsletters, website and the school prospectus.
- From 2018, in KS2, the Google and Parentzone document 'Be Internet Legends' will be used to teach E-Safety.

E-Safety information for parents/carers

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child (FS / KS1 agreement and KS2 agreement).
- 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.)

- The school website contains useful information and links to sites like Thinkuknow, Childline

Password Security

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.
- Adult users are provided with an individual network and email. (Also Learning Platform log-in username in future.)
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others. If you think your password may have been compromised or someone else has become aware of your password report this to Carol Walsh, School Business Manager
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems (and/or Learning Platform,) including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

Data Security

The accessing of school data is something that the school takes very seriously.

- Staff are aware of their responsibility when accessing school data. They must ensure that any data they access is properly protected, both on and off school site.
- All removable hardware containing information regarding the school must be encrypted and secured with strong passwords, that are not shared with anybody else.

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the Yorkshire & Humberside Grid for Learning (YHGfL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected, it will be followed up.

- The school maintains pupils will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources. All users must observe copyright of materials from electronic resources.

Infrastucture

- Doncaster Local Authority has a monitoring solution via the Yorkshire & Humberside Grid for Learning where web-based activity is monitored and recorded.
- School internet access is controlled through the LA's web filtering service. For further information relating to filtering please go to http://www.yhgfl.net/eSafety/Schools/Infrastructure
- Barnby Dun Primary is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 2018, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to internet logs.
- The school uses management control tools for controlling and monitoring workstations.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety co-ordinator.
- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network manager's to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media, it must be given to the teacher for a safety check first.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Headteacher, who will decide if the network technician should install it.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed through the ICT problems log book. The YHGfL Virus Outbreak Policy must be followed.
- All removable hardware and laptops must be encrypted and only accessed using individual passwords.

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 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.

Publishing pupils' images and work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school web site, prospectus, displays around school etc. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, safeguarding issues etc.
- Parents/ carers may withdraw permission, in writing, at any time.
- Pupils' names will not be used on the Web site or Blog, in association with photographs.
- Parents will be asked for consent when photographs are to be used or taken by the press because their circulation and coverage may be local, national and sometimes international.
- Pupil's work can only be published with the permission of the pupil and parents and will not enable them to be individually identified.

Photographs taken by parents/carers for personal use

- In the event of parents/carers wanting to take photographs for their own personal use, the school will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner, including use on personal websites or any form of social media (e.g. school plays)

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 and parents will be advised that the use of social network spaces outside school is illegal for primary aged pupils, although we acknowledge pupils may encounter such sites, with older siblings. Parents are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school.
- School staff are strictly advised not to add children or parents as 'friends' if they use social media sites (Staff Code of Conduct).

Staff private use of social media

- No reference should be made in social media to students / pupils, parents / carers / school staff or issues / situations related to the school.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles should be regularly checked to minimise risk of loss of personal information.

Mobile technologies

- Many new and existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside school. Some now offer open access to the internet and therefore open up risks associated with unregulated internet access.
- Emerging technologies will be examined for educational benefit and the risks assessed before use in school is allowed.
- The school allows staff to bring in personal mobile phones and devices for their own use, as long as the 'Mobile phone agreement' is signed and adhered to.

- Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device, unless circumstances offer no other option e.g. on a residential visit; in such a case, a staff's personal number will be withheld.
- Pupils are not allowed to bring personal mobile devices/phones to school; any child that needs to contact their parents will be given access to a school phone. Any phones that are brought in will be looked after by the office staff until the end of day.

Managing video-conferencing (future)

- When it is introduced into our school, IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety, for example if it is used for adult or family learning courses.

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 DMBC 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 Headteacher.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety co-ordinator.
- Depending on the seriousness of the offence, investigation by the Headteacher/ LA may involve immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and KCSIE 2018.
- Pupils and parents will be informed of the complaints procedure.

The e-Safety Policy and its implementation will be reviewed annually.

September 2018 - CM