HILLSIDE ACADEMY

e-safety Policy

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 provide pupils 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

Much ICT, however, particularly web-based resources, are not consistently policed and so all users need to be aware of the range of risks associated with the use of these internet technologies.

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: and technologies owned by staff, but brought onto school premises.

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 coordinator in our school is Belinda Fowler, subject leader in ICT. It is the role of the e-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as Doncaster LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the head/ e-Safety 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 should be read in conjunction with the following school policies: Child Protection, Health and Safety, Behaviour (including the anti-bullying) and PHSE & C.

e-Safety skills development for staff

- Staff receive regular updates information on e-Safety issues through the co-ordinator.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.
- 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 will be available on the school website.

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 may be 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 this. 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 report abuse button).
- 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.

e-Safety information for parents/carers

- 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.)
- The school will offer an information session for parents/carers once a year.

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.
- Pupils are not allowed to deliberately access files on the school network, of teachers or others. They may be given permission by their teacher to access the files of other pupils in their class.
- If a member of staff thinks that her password may have been compromised or someone else has become aware of it report this to the School Office 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 every 60 days. Individual staff users must also make sure that workstations are locked when left unattended.

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 not;

  o access data outside of school
  o take copies of the data
  o allow others to view the data
  o edit the data unless specifically requested to do so by the Principal and/ or Governing Body.

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.

- 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
- Staff and pupils are aware that school based e-mail and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to internet logs.
- If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the eSafety co-ordinator.
- It is the responsibility of the school, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.
- Software can only be installed by either technical support and subject leader, with permission of the Principal.
- 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 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.
- If there are any issues related to viruses or anti-virus software, technical support should be informed, immediately.

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 website, 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, eg divorce of parents or custody issues,
- Parents/ carers may withdraw permission, in writing, at any time.
- Pupils' names will not be used anywhere on the website or blog, particularly 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.
- Pupils' 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, (eg school plays), 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.

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 inappropriate for primary aged pupils. However we accept that some pupils will still use them; they will be advised never to give out personal details of any kind which may identify them or their location.
- Our pupils are asked to report any incidents of bullying to the school.
- School staff are advised not to add children as 'friends' if they use these sites. (Staff Code of Conduct)

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.
- Pupils are not allowed to bring personal mobile 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 class teacher until the end of day.

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 Principal.
- 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 Principal/ Academy Trust may involve immediate suspension, possibly leading to dismissal and, for very serious offences, involvement of the police.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.