High Crags Academy

High C
Acade

High Crags Academy

Rationale

Harnessing Technology: Transforming learning and children's services sets out the Government plans for taking a strategic approach to the future development of ICT.

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners. To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom."
DfES, eStrategy 2005

E-Safety

At High Crags, we recognise our duty to ensure that every child in our care is safe, and believe the same principles apply to the 'virtual' or digital world as would be applied to the school's physical environment. This Policy document is drawn up to protect all parties – the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

Aims

This eSafety/Internet Access Policy outlines how Internet use supports the educational aims of High Crags Primary School. This policy will be reviewed on a bi-annual basis. The purpose of Internet Access at High Crags is to raise educational standards, to support professional work and to enhance the school's management information and business administration systems. School Internet use is increasing and it is becoming an important part of learning and communication across all curricular areas and is an invaluable tool in the development of life long learning skills. Children and teachers at High Crags have access to a range of online materials that enrich and extend teaching and learning opportunities.

The benefits to teaching and learning include:
• Access to world-wide educational resources including museums and art galleries;
• Information and possible cultural exchanges between pupils nationally and world-wide;
• Access to news and current affairs;
• Access to educational materials and learning resources;

However, internet access is an entitlement for pupils based on responsible use. Children will be taught from an early age that they are responsible for their actions on the internet. At Key Stage 2 children are required to complete a Pupils Responsible Use Form. Each September, KS2 children will be taught or reminded about the rules of e-Safety. Internet access will be carefully planned to enrich and extend learning opportunities as an integrated aspect of the curriculum. Pupils will be given clear objectives for Internet use and will access material under guidance from their class teacher. Teachers will supervise pupils and take all reasonable precautions to ensure that users only access material appropriate to their learning. Parents are informed that pupils will be provided with internet access to support their learning and parents are required to sign a Parental Consent Form.

Internet use

The school's Internet access will be designed exclusively for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Pupils will be educated in the effective use of the Internet for research purposes, including the skills of information location, retrieval and evaluation. When appropriate the school will use 'safer' search engines with pupils such as *www.askforkids.com* or *www.yahooligans.com* or alternative online resources such as Espresso to support pupils in locating and retrieving information.

Managing Internet Access and Information system security

At High Crags, we:

• Maintain a broadband connectivity through the Bradford Learning Network (BLN) and so connect to the National Education Network. We use the Synetrix Netsweeper BLN filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature. Staff and students are aware that they must report any failure of the filtering systems directly to the ICT Coordinator. Our systems administrator will block any sites deemed necessary and report them to the LA / BLN where necessary.
• Ensure virus protection is updated regularly.
• Use separate log-in areas for pupils, teachers and visitors/parents.
• Block all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform.
• Only use BLN recommendations for pupil's own online creative areas such as web space and ePortfolio.
• Only use approved discussion sites, such as those on the BLN approved Learning Platform and block others.

The Technologies

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 (MSN/Yahoo etc.) often using simple web cams
• Blogs (an on-line interactive diary)
• Podcasting (radio/audio broadcasts downloaded to computer or MP3/4 player)
• Social networking sites (Myspace/Bebo/Facebook etc.)
• Video broadcasting sites (Youtube etc.)
• Chat Rooms
• Gaming Sites (Runescape etc.)
• Music download sites (Limewire/iTunes etc.)
• Mobile phones with camera and video functionality
• Smart phones with web functionality and emailing
(Please see the Glossary at the back of this policy for further definitions.)

Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements here at High Crags Primary School:
• An effective range of technological tools
• Policies and procedures, with clear roles and responsibilities
• A comprehensive e-Safety policy for pupils, staff and parents

Roles and Responsibilities

E-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 Headteacher ensures that the Policy is implemented and monitored. The responsibility for e-Safety has been designated to a member of the senior management team. The Deputy Head and the ICT Coordinator are our e-Safety Co-ordinators. Our e-Safety Coordinators ensure they keep up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Department and through organisations including The Child Exploitation and Online Protection (CEOP). The school's e-Safety coordinators ensures that the Headteacher, senior management and Governors are updated as necessary. Governors need to have an understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on e-Safety and are updated at least annually on policy developments. All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools' Policy including:
• Safe use of e-mail;
• Safe use of Internet
• Safe use of school network, equipment and data;
• Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
• Publication of pupil information/photographs and use of website;
• eBullying / Cyberbullying procedures;
• Their role in providing e-Safety education for pupils;
• Staff are reminded/updated about e-Safety matters at least once a year.

How will complaints regarding E-Safety be handled?

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. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.
Staff and pupils are given information about infringements in use and possible consequences:
• Discussion with e-Safety Coordinator / Headteacher
• Informing parents or carers
• Removal of Internet or computer access for a period
• In severe cases, referral to LA / Police
Our e-Safety Coordinators act as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher. Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Monitoring and Review

This Policy has been approved by the Governing Body and will be reviewed annually in consultation with the school leadership team and school staff. The policy is available to parents and the wider community. The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection. The e-Safety Policy and its implementation will be reviewed as and when new guidance is provided, approved by the Chair of Governors. A full review will be conducted annually

At High Crags:

- We ensure all pupils, staff and visitors, read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- We teach e-Safety to all pupils in Key Stage 2, every September, using the necessary guidance laid down by appropriate agencies.
- We teach pupils how to evaluate Internet content and to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- We encourage pupils to tell a teacher/responsible adult immediately if they encounter any material that makes them feel uncomfortable.
- We ensure pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or e-safety/ICT co-ordinator.
- We ensure pupils and staff know what to do if a cyber-bullying or other e-safety incident occurs.

Email

- Pupils only use BLN 'Imail' emailing system.
- Pupils can only use the e-mail accounts prepared for them on the school webmail.
- Pupils are introduced to, and use e-mail as part of the ICT scheme of work.
- 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.
- Whole class or group e-mail addresses are used in school
- Access in school to external personal e-mail accounts may be blocked, due to restrictions to some sites.
- E-mail sent to external organisations 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.
- Members of staff must not send/receive emails which are known to be abusive or offensive.

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school learning platform.
- Work can only be published with the permission of the pupil and parents.
- Digital images /video of pupils are stored in the teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication.
- Photographs of pupils MUST NOT be taken using personal mobile phones.
- Pupils are only able to publish to their own 'safe' web-portal on the BLN in school using the school's learning platform.
- Pupils are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work.
- Pupils are taught about how images can be abused in their eSafety education programme.
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school.

Social Networking/Instant Messaging (Including SMS Messaging)

- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space.Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Mobile phones will not be used for personal use during formal school time. Any mobile phones brought into school must be given to the child's teacher immediately on arrival.
- The school is ***not*** responsible for any mobile phone equipment being looked after by any member of staff.
- Pupils will be advised about the consequences of sending abusive or inappropriate text messages.
- Staff must ensure, if they use social networking sites, that their profile is set to private and all communications on any such sites should be deemed professional and responsible at all times.

Published Content and the School Learning Platform

- The contact details on the School Learning Platform site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Using the School Network and System

The school:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet and email access.
- Provides staff/pupils/visitors with a group network username for their own separate network areas.

- Makes clear that pupils should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could delete files or change network settings.
- Makes clear that no pupil should look in another pupil's folder or alter someone else's work in any way.
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.
- Requires all users to always save their work and close all relevant windows/documents when they have finished working or are leaving a computer unattended.
- Requests children should always log-off and then log back on if they find a logged on machine which is not in their user group.
- Will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Makes clear that all staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities.
- All Visitors must sign the Visitors AUP before using any of the schools technological resources.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection is installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

Protecting Personal Data

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

Assessing Risks

- 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.

Handling E-safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse will be referred to the headteacher.
- 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.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms.
- 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 is essential at all times.

Parents

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Learning Platform/Website.

Glossary of Terms

TERM DEFINITION

Acceptable Use Policy (AUP)
A policy that a user must agree to abide by in order to gain access to a network or the internet. In the school context, it may also cover how other communication devices, such as mobile or camera phones, can be used on the school, premises.

Blog
A blog, also known as a weblog, is a form of online diary or journal. Blogs contain short frequently updated posts, arranged chronologically with the most recently posted item appearing at the top of the page. In addition to text, blogs can contain, photos, images, sound, video, archives and related links, and can incorporate comments from visitors.

Chatroom
A place where a user can communicate with people more or less instantaneously by typing messages which then appear on your computer screen, and are transmitted across the internet to be read by everyone else participating in the chat at that time. The conversation continues through the exchange of messages. Chat can either be moderated or unmoderated. In the latter case the conversation will be completely unsupervised. It is very easy to fake an identity when participating in a chat so be especially wary.

Discussion Forum/Messageboard
A discussion site on the internet, often focusing on a special theme. People can post messages online using the formats specified by the provider of this service. Some discussion forums require registration. Some forums contain an archive, which you can use to search for a given topic. Some forums are moderated where the administrator of the forum has the right to delete or edit any messages posted. or to ban abusive users.

Email Groups /Mailing List
Email mailing lists on specific topics that users can subscribe to. Once subscribed the user receives all the messages sent to the group and anything the user sends in is similarly distributed. It is mainly used to conduct discussions about the topic of the mailing list.

Filtering
A method used to prevent or block users' access to unsuitable material on the internet.

Firewall
A network security system used to restrict internal and external traffic.

Hacking
The process of illegally breaking into someone else's computer system, reaching the computer's security.

Information Literacy/ Digital Literacy
The ability to locate pertinent information, evaluate its reliability, analyse and synthesise it to construct personal meaning and apply it to informed decision making.

Instant Messaging
A form of live chat. Generally a user joins a service (most popular is MSN) and then whenever they log on to the internet their name will appear in a central register. The user can then be contacted by anyone on the register and added to that person's contact list, although they will, of course, have to agree to accept their call. A user's email address must be known before they can be added to someone's list of contacts. With some of the more popular forms of instant messaging a user can join a club and all members of the club are notified when any other member logs on.

International Mobile Equipment Identity (IMEI)
A unique 15-digit serial number for mobile phones. When a phone is lost or stolen the number can be identified as invalid, so rendering the handset useless. It can be found by keying *#06# on your phone's keypad.

Internet Service Provider (ISP)
A company providing a connection to the internet and other services, such as browser software, email, a helpline, web space and subscriber-only content.

Newsgroups
Like an electronic bulletin board where people with common interests can keep in touch and up to date. You post to the newsgroup using a newsreader, a basic newsreader is included in Outlook Express. Newsgroups can also include video and music files for download.

Parental Control Software
Programmes that allow parents or other responsible adults to control various aspects of how a particular computer or network might interact with the internet. Some internet service providers offer free parental control software to members.

Peer-to-Peer (P2P)
P2P software allows users to search for files (such as music or videos) in specific folders of other users who are connected to the software. And therefore, also allows others to search the user's specified folders. These files are mostly copyrighted material and so illegal to download unless the user already owns a legally purchased copy. P2P networks are also littered with viruses.

Personal Digital Assistant (PDA)
A small, mobile, handheld device that provides computing and information storage/retrieval capabilities, and possibly phone facilities too.

Podcast
An audio file which can contain music, speaking or a mixture of the two. Can be made by anyone from large companies like the BBC to non-professional individuals. They can be downloaded and played through iTunes or on an iPod.

Pop-Up
A new window that opens on top of the active internet browser window. This window does not usually contain it's own web address, however in some cases it can do. Pop-ups that open without the user's request usually contain advertisements. Pop-up blockers are available as part of most browsers.

Sexting
Taking sexually explicit photos using a portable device such as a mobile phone and forwarding the pictures by text/picture message.

SMS Text Messaging.
The acronym SMS stands for short message service. SMS messaging allows for short text messages to be sent from one cell phone to another.

Social Networking Sites
Sites such as myspace or bebo which allow users to create an online profile that others can then search for and ask for permission to add that person to their list of friends. The online profile would usually include a photo, the user's age, gender, hometown and a list of their hobbies/favourite things. The user can also post a blog, music and video on their page. People on the user's friend list are allowed to send messages, leave comments or contact the user through instant messaging services.

Spam
Unsolicited junk email. The term is also used to describe junk text messages received via mobile phones. A related term SPIM (or spIM), describes receiving spam via instant messaging.

Spoofing
Assuming the identity of someone else, using an email address either guessed or harvested from repositories of valid email addresses (such as the address book of a virus infected computer). Spoofing is typically practised to veil the source of virus-laden emails, or, often, to obtain sensitive information from spam recipients, without revealing the source of the spammers.

URL
An abbreviation for uniform resource locator, or a web address.

Virus
A computer program that enters a computer, often via email, and carries out a malicious act. A virus in a computer can corrupt or wipe all information in the hard drive, including the system software. All users are advised to guard against this by installing anti-virus software.

Webcam
A webcam is a camera connected to a computer that is connected to the internet. A live picture is uploaded to a website from the camera at regular intervals, typically every few minutes. By looking at the website you can see what the camera sees – almost as it happens.