Hanwell Fields Community School
The best in everyone™
Part of United Learning

Hanwell Fields Community School
E-safety and Internet Access Policy

What is E-Safety?

The School's e-Safety Policy replaces the Internet Policy to reflect the need to raise awareness of the safety issues associated with information systems and electronic communications as a whole.

E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Who will write and review the policy?

The E-Safety Policy is part of the ICT Policy and School Development Plan and should relate to other policies including those for behaviour, personal, social and health education (PSHE) and for citizenship. Policy construction provides a method to review practice, in this case the use of a major technology and its benefits and risks. The more that staff, parents, governors and pupils are involved in deciding the policy, the more effective it will be.

- Our E-Safety Policy has been written by the school, building on government guidance. It has been agreed by the senior management and approved by governors.
- The school will appoint an E-Safety Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap.
- The E-Safety Policy and its implementation will be reviewed annually.

Why is Internet use important?

The rapid developments in electronic communications are having many effects, some profound, on society. Only ten years ago we were asking whether the Internet should be used in all schools. Now every pupil is younger than the World Wide Web and many use it more than their teachers. Nevertheless it is important to state what we are trying to achieve in education through ICT and Internet use.

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with United Learning, Oxfordshire County Council and EXA (Broadband provider) and DfES;
- access to learning wherever and whenever convenient.

How can Internet use enhance learning?

Increased computer numbers or improved Internet access may be provided but learning outcomes must also be addressed. Developing effective practice in Internet use for teaching and learning is essential. Teachers can help pupils to learn how to distil the meaning from the mass of information provided by the Internet. Often the quantity of information is overwhelming and staff may guide pupils to appropriate websites, or teach search skills. Offering younger pupils a few good sites is often more effective than an Internet search. Above all pupils need to learn to evaluate everything they read and to refine their own publishing and communications with others via the Internet.

- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

How will pupils learn how to evaluate Internet content?

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop skills in selection and evaluation. The spreading of malicious rumour has occurred for thousands of years and lies can win over truth. Information received via the Internet, e-mail or text message requires good information handling skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues present with books or TV may be missing or difficult to read. A whole curriculum approach may be required.

Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: to close the page and report the incident immediately to the teacher. More often, pupils will be judging reasonable material but will need to select relevant sections. Pupils should be taught research techniques including the use of subject catalogues and search engines and be encouraged to question the validity, currency and origins of information. Key information handling skills include establishing the author's name, date of revision and whether others link to the site.

Pupils should compare web material with other sources. Effective guided use will also reduce the opportunity pupils have for exploring unsavoury areas.

Clearly pupils need to understand that unselective copying is worth little without a commentary that demonstrates the selectivity used and evaluates significance. Respect for copyright and intellectual property rights, and the correct use of published material should be taught. Methods to detect plagiarism may need to be further developed and are certainly part of examination boards' thinking.

The following statements require adaptation according to the pupils' age:

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

The evaluation of on-line materials is a part of every subject.

How will e-mail be managed?

E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects between schools in neighbouring villages and in different continents can be created.

The implications of e-mail use for the school and pupils need to be thought through and appropriate safety measures put in place. Un-regulated e-mail can provide routes to pupils that bypass the traditional school boundaries.

- Access in school to external personal e-mail accounts may be blocked.
- Pupils may only use approved e-mail accounts.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Whole-class or group e-mail addresses should be used
- Excessive social e-mail use can interfere with learning and may be restricted.
- 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.

How will published content be managed?

Sensitive information about schools and pupils could be found from a newsletter but a school's website is more widely available. Publication of information should be considered from a personal and school security viewpoint. Material such as staff lists or a school plan may be better published in the school handbook or on a secure part of the website which requires authentication.

- E-mail addresses should be published carefully, to avoid spam harvesting.
- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Can pupil's images or work be published?

Still and moving images and sounds add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount. The publishing of pupils' names with their images is not acceptable. Published images could be re-used, particularly if large images of individual pupils are shown.

Strategies include using relatively small images of groups of pupils and possibly even using images that do not show faces at all. "Over the shoulder" can replace "passport-style" photographs but still convey the educational activity. Personal photographs can be replaced with self-portraits or images of pupils' work or of a team activity. Pupils in photographs should, of course, be appropriately clothed.

- Work can only be published with the permission of the pupil and parents.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs
- Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Written permission from parents or carers will be obtained before images of pupils are electronically published.

How will social networking and personal publishing be managed?

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control.

For use by responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published.

Examples include: Facebook, blogs, wikis, MySpace, Bebo, Piczo, Windows Live Spaces, MSN space, forums, bulletin boards, multi-player online gaming, chatrooms, instant messenger and many others.

- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- The schools will block/filter access to social networking sites
- Students should be advised not to publish specific and detailed private thoughts.
- Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

How will filtering be managed?

Levels of Internet access and supervision will vary according to the pupil's age and experience. Internet access must be appropriate for all members of the school community. The technical strategies being developed to restrict access to inappropriate material fall into several overlapping types (commonly described as filtering):

- Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.
- A walled-garden or "allow-list" restricts access to a list of approved sites. Such lists inevitably limit pupils' access to a narrow range of information.
- Dynamic filtering examines web page content or e-mail for unsuitable words. Filtering of outgoing information such as web searches is also required.
- Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject these pages.
- Access monitoring records the Internet sites visited by individual users. Attempted access to a site forbidden by the policy will result in a report.
- The school will work with United Learning and Oxfordshire County Council and EXA (Broadband supplier) to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL must be reported to the e-Safety Coordinator.

How will videoconferencing be managed?

Videoconferencing enables users to see and hear each other between different locations. It is a 'real time' interactive technology and has many uses in education.

Equipment ranges from small PC systems (web cameras) to large room based systems that can be used for whole classes or lectures. The videoconferencing equipment uses a 'network' to communicate with the other site.

Videoconferencing now uses IP networks. All modern standards-based videoconferencing systems will connect over IP. However, videoconferencing over the Internet, even with a broadband connection, can be unpredictable since it is a shared network and quality of service cannot be controlled. Schools using the Internet for videoconferencing should be aware that it is not managed by a single responsible agency and that there is no inherent security.

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses should not be made available to other sites.
- Videoconferencing contact information should not be put on the school Website.
- The equipment must be secure and if necessary locked away when not in use.
- School videoconferencing equipment should not be taken off school premises without permission. Use over the non-educational network cannot be monitored or controlled.
- Parents and guardians should agree for their children to take part in videoconferences, probably in the annual return.
- Responsibility for the use of the videoconferencing equipment outside school time needs to be established with care.
- Only key administrators should be given access to the videoconferencing system, web or other remote control page available on larger systems.

- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.
- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference.

- Recorded material shall be stored securely.
- If third-party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class.

How can emerging technologies be managed?

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, wide Internet access and multimedia. A risk assessment needs to be undertaken on each new technology and effective practice in classroom use developed. The safest approach is to deny access until a risk assessment has been completed and safety demonstrated.

Even e-mail should be considered an emerging technology until rules have been set. E-mail can be sufficient to set up a virtual community. The pupils in two schools could create a shared project using class e-mail and a common website or blog. Staff and governors make a larger community, which could be extended to include parents.

Video conferencing introduces new dimensions. Web cameras cost as little as £50 and, with faster Internet access, can enable limited video to be exchanged across the Internet. The availability of live video can increase safety – you can see who you are talking to – but if inappropriately used, a video link could reveal security details.

New applications are continually being developed based on the Internet, the mobile phone network, wireless or infrared connections.

How will Internet access be authorised?

The school should allocate Internet access for staff and pupils on the basis of educational need. It should be clear who has Internet access and who has not. Authorisation is generally on an a group basis, where pupil usage is fully supervised, all pupils in a class could be authorised as a group.

- Parents will be informed that pupils will be provided with supervised Internet access
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

How will risks be assessed?

As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will need to address the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the school system.

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor EXA (broadband supplier) can accept liability for the material accessed, or any consequences resulting from Internet use.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- Methods to identify, assess and minimise risks will be reviewed regularly.

How will e-safety complaints be handled?

Parents, teachers and pupils should know how to submit a complaint. Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance whether the Internet use was within or outside school.

A minor transgression of the rules may be dealt with by the teacher. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's disciplinary policy. Potential child protection or illegal issues must be referred to the school Designated Child Protection Coordinator or e-Safety Coordinator. Advice on dealing with illegal use could be discussed with the local Police Youth Crime Reduction Officer.

- Pupils and parents will be informed of the complaints procedure.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Sanctions within the school discipline policy include:
  - interview/counselling by the head of year;
  - informing parents or carers;
  - removal of Internet or computer access for a period.

Please ensure that this Policy is cross referenced with United Learning Guidance regarding E Safety: https://biecloud.csco.org.uk/

Reviewed: April 2013 **Next review: 2016**