HENLEY-in-ARDEN SCHOOL

Online Safety, Internet and Acceptable Use of IT Policy

arts colleges

Updated: October 2014

Approved by Governors: December 2014

Review: November 2017

Why Internet Use is Important

The rapid developments in electronic communications are having many effects, some profound, on society. Only a few years ago we were asking whether the Internet should be used in all schools. Now every pupil is younger than `he 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.

Benefits of the Internet to education

All Warwickshire schools have access to Broadband Internet connections. A number of studies and government projects have identified the benefits to be gained through the appropriate use of the Internet. These benefits are outlined in the possible statements for inclusion in the policy:

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries and to experts in many fields for pupils and staff;
- inclusion in the National Education Network connecting all UK schools; educational and cultural exchanges between pupils world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- 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
- access to learning wherever and whenever convenient.

How the Internet enhances 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. Librarians and 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.

The school Internet access will be designed expressly for pupil use and will be filtered appropriately.

Pupils will be taught what Internet use is acceptable and what is not and will be given clear objectives for Internet use.

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.

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.

Pupils

Many pupils are very familiar with Internet use and culture and it is good practice to design elements of the School online safety Policy with them, possibly through the student council and PSHCE (Personal, social, health and citizenship education) lessons. As pupils' perceptions of the risks will vary, the rules for responsible use will need explanation and discussion. Pupils will need to be reminded of the school rules. Rules for Internet access will be posted in all networked rooms.

Pupils will be informed that Internet use will be monitored.

An online safety training programme will be delivered to all pupils to raise the awareness and importance of safe and responsible use of the Internet and other electronic communications tools.

This programme will focus on PSHE and ICT areas of learning.

Instruction in responsible and safe use should precede Internet access and should be reinforced at regular intervals.

A module on responsible Internet use will be included in the PSHE, Citizenship and ICT programmes covering both school and home use.

Staff

This policy will only be effective if all staff subscribe to its values and methods. Staff will be given opportunities to discuss the issues and develop appropriate teaching strategies. All staff will be given the School online 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.

Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Staff development in safe and responsible Internet use and on the school online safety Policy will be provided as required.

Parents

Internet use in pupils' homes is now very widespread. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school may be able to help parents plan appropriate, supervised use of the Internet at home. Parents should also be advised to check if pupils' use elsewhere is covered by an appropriate use policy.

Parents' attention will be drawn to the School online safety Policy in newsletters, the school brochure and on the school Website.

Internet issues will be handled sensitively to inform parents without alarm.

A partnership approach with parents will be encouraged.

Interested parents will be referred to organisations listed in the section on online safety Contacts and References

Pupils evaluating Internet content

Information received via the Internet, email or text message requires good information handling skills. 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 to evaluating information may be required. Pupils should be taught research techniques and key information handling skills

Pupils may occasionally be confronted with inappropriate material, despite filtering. They will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. Access to sensitive sites, for example those that record the Holocaust, may be required for the duration of a specific educational activity by supervised pupils of appropriate age.

Pupils need to understand how to extract, interpret and use information and evaluate its 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 developed.

The schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the Senior ICT Technician, and where appropriate the school online safety officer.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

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.

Publishing images of staff and pupils

Photographs that include pupils and/or staff add a liveliness and interest to a website. Nevertheless the security of staff and pupils must come first. The publishing of pupils' full names with their photographs is not acceptable. Web images could be misused and individual staff and pupils identified unless broad descriptions are used.

Strategies include using relatively small photographs of groups of pupils and using photographs that do not show faces such as over the shoulder photographs. Paintings/drawings or images of pupils' work or of an activity can also replace photographs. A check should be made that pupils in photographs are appropriately clothed.

Photographs of a pupil should not be published without the parent's or carer's written permission. The school will ask for permission to publish images of work or appropriately taken photographs of pupils on entry to the school.

Similarly, photographs of school staff should not be published without consent.

Pupils need to be taught the reasons for caution in publishing personal information and photographs in social publishing sites

Managing social networking

Social networking sites can connect people with others for a wide range of purposes, including educational purposes. Guests can be invited to view personal space, pupils' work or documents and leave comments. There is increasing educational use of such tools, for example in the use of blogs and wikis to improve writing. Social networking has many possibilities for staff and pupils working together and is increasingly used in an educational context.

A significant proportion of pupils in secondary schools now use social networking out of school hours on a regular basis. They need guidance and support in knowing how to stay safe on such sites and parents may not know what advice to give them.

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.

Social networking sites can be used to bully others. Schools should ensure that pupils know what to do if they are bullied using social networking sites. Although most social networking

sites are used outside school, the school has a responsibility along with parents to ensure that incidents of bullying are resolved.

The use of communications tools is blurring the boundaries between home and school, both in 'earning and in the use of social networking. Schools have a responsibility to deal with incidents that take place after school if they involve school networks. They also have some responsibility to work with parents to prevent and to resolve incidents that involve mobile phones or other social networking sites.

Social networking sites and newsgroups will be blocked unless a specific use is approved.

Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, email address, names of friends, specific interests and clubs etc.

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 will be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name, school or shopping centre.

Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should not run social network spaces for students on a personal basis. Teachers should not communicate with pupils through private social networking sites, even on educational matters, but should use official sites sanctioned by the school.

Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others. They 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. Incidents of bullying through social networking will be dealt with in line with the school policy on bullying.

Managing Filtering

Levels of access and supervision should vary according to the pupil's age and experience. Internet access must be appropriate for all members of the school community and systems should be in place to adapt the access level according to pupils' specific areas of study are available and to meet staff needs.

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

Managing filtering is the responsibility of the ICT technician

Managing Email

Email use can bring significant educational benefits and interesting projects between neighbouring villages or towns and even continents can be created. However, un-regulated email can provide

routes to pupils that bypass the traditional school boundaries and spam, phishing and virus attachment can make email risky. As with social networking, email can be used to bully others and the school has a responsibility, along with parents, to ensure that incidents of bullying are resolved.

In the school context, email should not be considered private and most schools and many firms reserve the right to monitor email. There is a balance to be achieved between necessary monitoring to maintain the safety of pupils and the preservation of privacy, both of which are covered by legislation.

- A central question is the degree of responsibility that can be delegated to individual pupils. Restriction of incoming and outgoing email to approved addresses and filtering for unsuitable content and viruses is now possible. Schools should consider banning access to external web-based email, particularly as anonymous identities such as pjb354emailhost.com make monitoring difficult. Strategies include limiting pupils to email accounts on the school domain or restricting email traffic to the school domain.

- Pupils may only use approved email accounts on the school system.

- Pupils must immediately tell a teacher if they receive offensive email.

- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.

- Use of words included in the filtering/checking 'banned' list will be detected and logged.

- Access in school to external personal email accounts may be blocked.

- Excessive social email use can interfere with learning and may be restricted.

- Email 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.

- Email addresses should be published carefully, to avoid spam harvesting.

Video Conferencing (including Internet telephony such as Skype)

Video conferencing 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 video conferencing equipment uses a 'network' to communicate with the other site.

Video conferencing introduces new dimensions. Web cameras 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.

Schools with full 'DfE Specification' broadband are connected through the LA and Regional Broadband Consortia and have access to services such as gatekeepers and gateways to enable schools to communicate with other locations outside their LA. MCUs (Multipoint Control Units) enable several schools to communicate at one time, for instance with several video streams each.

- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- IP video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- 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.
- Video conferencing contact information should not be put on the school website
- School video conferencing equipment should not be taken off school premises without permission. Use over the non-educational network cannot be monitored or controlled.
- The equipment must be secure and if necessary locked away when not in use.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Video conferencing should be supervised appropriately for the pupils' age.
- Responsibility for the use of the video conferencing equipment outside school time needs to be established with care.
- Only key administrators should be given access to the video conferencing system web or other remote control page available on larger systems.
- Unique log on and password details for the educational video conferencing services should only be issued to members of staff and kept secure.
- When recording a 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 owners' Intellectual Property Rights (IPR).
- Video conferencing 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 the class.

Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools. A risk assessment needs to be undertaken on each new technology, and effective

practice in classroom use should be developed. The safest approach is to deny or severely control and restrict access until a Risk Assessment has been completed and safety demonstrated.

Virtual classrooms and virtual communities widen the geographical boundaries of learning. New requirements for online reporting to parents are being introduced. On-line communities may encourage a disaffected pupil to keep in touch or provide access to learning for an isolated pupil. The safety and effectiveness of wider virtual communities depends on users being trusted and identifiable. This may not be easy, as authentication beyond the school may be difficult as demonstrated by social networking sites. The registering of individuals to establish and maintain validated electronic identities is an important part of the process.

New applications are continually being developed based on the Internet, the mobile phone network, wireless or infrared connections. Wireless access has increased the mobility and range of access. This has led to a number of issues such as the videoing of teachers and the publication of the videos on social networking sites. The Schools will consider appropriate responses to this type of behaviour.

Schools should keep up to date with new technologies and communication methods and be ready to develop appropriate strategies. For instance text messaging is a frequent activity for many pupils that could be used for both appropriate and inappropriate activity in schools.

The inclusion of inappropriate language or graphical icons within text messages is difficult for staff to detect. Pupils need reminding that such usage is both inappropriate and conflicts with school policy. Abusive text messages will be dealt with under the school anti bullying policy.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

- There is a policy on phone use in school.

- Staff will be issued with a school phone where contact with pupils is required.

Managing Information Services

Information management is a complex and multi-faceted set of processes and cannot be dealt .with adequately in this document. This is a major responsibility that includes delivery of essential services and has implications for the personal safety of staff and pupils. There is a policy on Information handling

- Effective information management requires a combination of robust technical systems and appropriate behaviour by the user. The most sophisticated information security system can be completely undermined by the member of staff who leaves the system logged on and unattended whilst they are distracted by something.

- A number of agencies can advise on security including Becta and Warwickshire's Information Strategy Manager.

- Local Area Network security issues include:

- Users must act reasonably - the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for network use. Disregarding ICT usage policy is regarded as a matter for disciplinary procedures.
- Workstations should be secure from deliberate or opportunistic access by unauthorised users.
- Servers must be located securely and physical access restricted.
- The server operating system must be secure and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be pro-actively managed and conform to technical standards recommended by Becta.
- All Internet connections through Warwickshire Broadband will ensure compliance with the security policy.
- Warwickshire Broadband firewalls and switches are configured to prevent unauthorised access between schools.
- Decisions on WAN security are made on a partnership basis between school and Warwickshire Broadband.
- Action points for the school
- The security of the school information systems will be reviewed regularly. Virus protection will be updated regularly.
- Security strategies will follow Warwickshire MBC guidelines.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Portable media may not be used without specific permission followed by a virus check. Where they are used to store personal information they will be encrypted. Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT co-ordinator / network manager will review system capacity regularly.

Protecting Personal Data

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals.

Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify an individual).

The eight principles are that personal data must be:

1. Processed fairly and lawfully
2. Processed for specified purposes
3. Adequate, relevant and not excessive
4. Accurate and up-to-date
5. Held no longer than is necessary
6. Processed in line with individuals rights
7. Kept secure
8. Transferred only to other countries with suitable security measures.

The Information Commissioner's Office provides relevant information: http://www.ico.gov.uk/

Personal data will be recorded, processed, transferred and made available in compliance with to the Data Protection Act 1998.

Online safety Complaints

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 by pupils 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 Behaviour for Learning policy.

Complaints linked to staff should be dealt with by a senior member of staff. It is likely that most online safety complaints will be dealt with using the normal complaints processes for the school. Potential child protection or illegal issues, however, must be referred to the school Designated Child Protection coordinator.

- Formal complaints of Internet misuse will be dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the head teacher who should use the agreed WCC procedures.
- Pupils and parents will be informed of the Complaints Policy
- Parents and pupils will need to work in partnership with staff to resolve issues.

Community use of ICT and the Internet

The Internet is available in many situations in the local community. In addition to the home,

access may be available at the library, youth club (HUB), adult education centre (Learning Resource), village hall, supermarket or cyber cafe. Ideally young people would encounter a consistent policy to Internet use wherever they are.

In community Internet access there is a fine balance to be achieved in ensuring 'freedom of information' whilst providing adequate protection for children and others who may be offended by inappropriate material. Each organisation will develop access appropriate to its own client croups and pupils may find variations in the rules and even unrestricted Internet access. Although policies and practices may differ, community partners adhere to the same laws as schools with respect to content, copyright and misuse. Staff may wish to exchange views and compare policies with others in the community. Where rules differ, a discussion with pupils on the reasons for the differences would be worthwhile. Pupils need to know how to stay safe online wherever they are.

Sensitive handling of cultural aspects is important. For instance filtering software may need to work across community languages and school Internet policies may need to reflect the pupils' cultural backgrounds. Assistance from the community in drawing up the policy could be helpful. Where appropriate:

- The school will liaise with local organisations to establish a common approach to online safety.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.