

# The Heath

## ICT Acceptable Use Protocol

### Introduction

The statutory curriculum requires students to learn how to locate, retrieve and exchange information using information and communications technology (ICT). In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail. In addition to this the development of online learning resources across the curriculum and the use of new technology in schools to enhance the learning experience and engage students mean that students are regularly engaged in activities which involve the use of ICT. Computer skills are vital to access life-long learning and employment; indeed we must consider ICT a life-skill.

The purpose of Internet use in The Heath School is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

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.

### Aim

The aim of this Acceptable Use Protocol (AUP) is to ensure that students will benefit from learning opportunities offered by the school's Internet resources in a safe and effective manner. Internet use and access is considered a school resource and privilege. Therefore, if the school's AUP is not adhered to this privilege will be withdrawn and appropriate sanctions will be imposed.

### The Internet and Learning

The Internet will enhance students' educational opportunities at The Heath School. Students, through Halton Local Authority infrastructure, can access the North West Learning Grid and the Joint Academic Network and take advantage of searching the World Wide Web and using e-mail.

### Benefits to Learning:

- Access to world-wide educational resources including museums and art galleries;
- Communication and collaboration between students and schools;
- Transfer of information between students and schools;
- Educational and cultural exchanges between students world-wide;
- Cultural, vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for students and staff;
- Staff professional development through access to national developments, educational materials and good curriculum practice;
- Communication with support services, professional associations and colleagues;
- Improved access to technical support including remote management of networks;
- Exchange of curriculum and administration data with the LA and DfES.

## **School Strategy**

The school will employ a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

### **General**

- Internet sessions during lesson time will always be supervised by a teacher. Adult supervision will be in place in the vicinity of student internet activity at breaktimes and other non-teaching times
- Filtering software and /or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material.
- The school will regularly monitor students' Internet usage.
- Students and teachers will be provided with training in the area of Internet safety.
- Uploading and downloading of non-approved software will not be permitted.
- Virus protection software will be used and updated on a regular basis.
- The use of personal USB devices in school requires a teacher's permission.
- Students will observe good "netiquette" (i.e., etiquette on the Internet) at all times and will not undertake any actions that may bring the school into disrepute.
- Supply teachers are not granted access to ICT.

### **Using the Internet in the Curriculum**

Initially, students will be educated about the Internet and its use in Computing lessons. During these sessions students will be taught research techniques and acceptable use. They should be encouraged to question the validity, currency and origins of information – key information handling skills. They should also use alternative sources of information for comparison purposes. They will also be educated to follow sensible rules for personal safety. Internet access will be planned to enrich and extend learning activities. The Internet will also be used in other subject areas in addition to Computing. Internet use is monitored by E-safe, a program running in the background as students work. Students are informed of this in the induction lessons or if joining later in the year by the designated safeguarding deputy. E-safe will create alerts if it presumes something outside of acceptable use has occurred and appropriate action will be taken.

### **Risk Assessment of Internet Materials**

As the quantity and breadth of the information available through the Internet continues to grow The Heath School realise that it is not possible to guard against every undesirable situation. However, in common with other media such as magazines, books and video, some material available via the Internet is unsuitable for students. 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 HBC can accept liability for the material accessed, or any consequences of Internet access. However, The Heath School will ensure that the methods used to identify, assess and minimise risks will be reviewed regularly. Similarly, staff, parents, and HBC will work to establish agreement that every reasonable measure is being taken.

### **World Wide Web**

- Students will not visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Students will use the Internet for educational purposes only.
- Students will be familiar with copyright issues relating to online learning.
- Students will never disclose or publicise personal information.

## **World Wide Web (Cont')**

- Students will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and /or network management reasons.
- Students will report any concerns or inappropriate materials to their teacher or the supervising member of staff.
- Students will not engage in illegal file sharing, including exchange or distribution of copyrighted, illegal or otherwise inappropriate material.

## **Email**

- Students will use approved class email accounts under supervision by or permission from a teacher.
- Students will not send or receive any material that is illegal, obscene, defamatory or that is intended to upset, annoy or intimidate another person.
- Students will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.
- Students will never arrange a face-to-face meeting with someone they only know through emails or the Internet.
- Students will note that sending and receiving email attachments is subject to permission from their teacher.

## **Internet Chat**

- Students will only have access to chat rooms, discussion forums or other electronic communication forums that have been approved by the school.
- Chat rooms, discussion forums and other electronic communication forums will only be used for educational purposes and will always be supervised.
- Usernames will be used to avoid disclosure of identity.
- Face-to-face meetings with someone organised via Internet chat will be forbidden.

## **Mobile Internet Technologies**

- Students will only use mobile internet hardware e.g. laptops, PDA's, webcams, digital cameras, under supervision and for legitimate subject related learning.
- Where students are issued with mobile technologies to support learning for a specific project these may be subject to a separate home/school agreement.

## **Digital Media/Image Capture and Storage**

- The use of digital media to capture and transfer images (camera phones or PDA's) is forbidden unless authorised by a member of staff and deemed appropriate technology for the planned learning activity.
- No information, image or digital video footage, gathered within The Heath or at a Heath event, is to be posted onto the internet without permission from the Principal. Images captured by staff or students must be used for an authorised purpose and not stored on personal devices.
- The use of digital media as a form of evidence to assess learning may be used in curriculum areas. This will only be shared with the relevant assessment bodies.

## **School Computers/Network**

- Users will not install any software without explicit permission.
- Users will not engage in any activity that compromises the security of the network.
- Users are to immediately report any damage or faults involving equipment or software, however this may have happened.
- Users will not try to obtain other people's personal information or passwords or access confidential data through hacking, use of malware or any other means.

## Mobile Phone Protocol

The use of mobile phones is not allowed at The Heath – however, it is understood that some students may carry them so that they can contact home after school. In this case the phone must be **switched off throughout the school day** including break and lunch time and kept out of sight at all times. If parents wish to contact their child during the day then they should phone school and a message will be passed to their child.

If a phone is seen or heard it will be **confiscated, taken to the front office, recorded, locked away and returned on Friday afternoon after school**. If a phone is confiscated on a Friday, it will be returned on the following Friday. This protocol has become necessary due to problems arising from widespread use of mobile phones in schools throughout the country. These have included the spreading of illegally taken images, illegal videoing and cyber-bullying. These can cause great distress in addition to the obvious interruption to teaching and learning.

## School Website

- Students will be given the opportunity to publish projects, artwork or school work on the World Wide Web.
- The publication of student work will be co-ordinated by a teacher.
- Students' work will appear in an educational context on Web pages with a copyright notice prohibiting the copying of such work without express written permission.
- Digital photographs, audio or video clips may be published on the school website as a record or celebration of events.
- Personal student information including home address and contact details will be omitted from school web pages.
- Students will continue to own the copyright on any work published.

The school will inform students and parents of key support structures and organisations that deal with illegal material or harmful use of the Internet.

## How will ICT system security be maintained?

The Heath School realise that it is important to review the security of the whole system, from user practice to Internet service provider (ISP). At the simplest level, occasional checks on user's files, temporary Internet files and history files can reveal potential mischief. A number of agencies can advise on systems security including LA support teams and suppliers. However, review of external agencies' opinions on systems security raises the following issues for further discussion:

### Local Area Network (LAN) security issues include:

- The user must act reasonably. Loading non-approved software could cause major problems. Good password practice is required including logout after use.
- Cabling should be secure and wireless LANs safe from interception.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured to a high level.
- Virus protection for the whole network must be installed and current.

### Wide Area Network (WAN) security issues include:

- All external connections must be assessed for security risks including the wide area network connection and any modems staff may wish to use.
- Firewalls and routers should be configured to prevent unauthorised use of software such as FTP and Telnet at the protocol level.
- Decisions on security made by external agencies such as the LA or ISP must be discussed with schools. Third-party security testing should be considered.

The Internet is a connection to the outside world that could compromise system performance or threaten user or system security. The downloading of large files such as video and MP3 can compromise system performance. A WAN connection introduces further risks such as students trying to access another school. However it also brings the opportunity for industrial strength security in the form of hardware firewalls and the expertise to design and operate them. Therefore:

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- E-Safe software is installed on the school network, this will track and monitor all student activity and will protect against risks associated with internet use
- Security strategies will be discussed with the LA, particularly where a wide area network connection is being planned.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Personal USB devices may not be used in school without specific permission from the teacher and a virus check.
- Unapproved system utilities and executable files will not be allowed in students' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.
- The ICT co-ordinator/network manager will ensure that the system has the capacity to take increased traffic caused by Internet use.

### **Handling Complaints**

Responsibility for handling incidents will be given to a senior member of staff through the faculty line manager hierarchy in The Heath School. Students will be informed of the process and parents and students will work in partnership to resolve any issue.

Any students found to be infringing the conditions laid down in the Conditions of Acceptable Use Protocol will be initially referred to the Head of ICT and, subsequently, dealt with by the school's sanctions procedures. Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases exclusion. The school also reserves the right to report any illegal activities to the appropriate authorities.

### **Legislation**

The school will provide information on the following legislation relating to use of the Internet which teachers, students and parents should familiarise themselves with:

- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video recordings Act 1989
- The Data Protection Act 1988