The Henry Prince First School

This policy is overarched and subject to the agreed contents and conditions of the Safeguarding Children and E-Esafety Policies

E-Safety Policy 2016

Introduction

The Internet is regarded as a crucial resource to support teaching and learning. The curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and mobile learning.

Computer skills are vital to access life-long learning and employment; indeed computing is now seen as an essential life-skill too. ICT skills and resources are used daily to support and enhance the learning of the children at The Henry Prince First School. Young people have access to the Internet from many places, such as home, school, friends' homes, libraries and in many cases mobile phones.

Schools have a number of services to help ensure that curriculum use is safe and appropriate, however, access out of school does not usually have these services and has a range of risks associated with its use. This policy is designed to ensure safe internet use by pupils in school and give them the skills and awareness to remain safe while on-line while out of school.

Rationale

The purpose of this policy is to:

- set out the key principles expected of all stakeholders of The Henry Prince First School with respect to the 'responsible' use of ICT-based technologies.
- safeguard and protect the children and staff of The Henry Prince First School.
- assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational or personal use.
- have clear structures to deal with online abuse, such as cyber-bullying, which are cross referenced with other school policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour, Including antisocial and/or extremist behaviour, is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

Our whole school approach to the safe use of ICT

Creating a safe, rich ICT learning experience that includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities to protect children and staff.
- E-Safety teaching is embedded into the school curriculum.

Technical and Hardware Guidance
School Internet provision:

The school uses a Staffordshire approved content filter to ensure that as far as possible, only appropriate content from the Internet finds its way into school. Whilst this filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter. In this case:
• All pupils and staff have been issued with clear guidelines on what to do if this happens, and parents will be informed where necessary.
• Pupils or staff who deliberately try and access unsuitable materials will be dealt with according to the rules outlined elsewhere in this document.

Downloading files and applications:

The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of school equipment.
• Pupils are not allowed to download any material from the Internet.

Portable storage media:

• Staff are allowed to use portable media storage (USB Keys etc) provided by the HT/Admin staff. If use of such a device results in an anti-virus message, they should remove the device immediately and report the incident to the ICT Leader and record the incident in the ICT Technician's log book.

Teaching and Learning

We think it is crucial to teach pupils how to use the Internet safely, both at school and at home, and we use the Kidsmart safety code to support our teaching in this area:

Kidsmart has been developed by the Childnet charity, and is endorsed by the DfES
http://www.kidsmart.org.uk
The main aspects of this approach include the following five **SMART** tips:
Safe - Staying safe involves being careful and not giving out your name, address, mobile phone no., school name or password to people online...
Meeting someone you meet in cyberspace can be dangerous. Only do so with your parents'/carers' permission **and** then when they are present...
Accepting e-mails or opening files from people you don't really know or trust can get you into trouble – they may contain viruses or nasty messages...
Remember someone online may be lying and not be who they say they are. If you feel uncomfortable when chatting or messaging end the conversation... (Xbox Live, PS4, FaceTime ….)
Tell your parent or carer if someone or something makes you feel uncomfortable or worried...

Why Internet use is important

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.
Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

• The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
• Pupils will be taught what Internet use is acceptable and when it is not.
• Internet access will be planned to enrich and extend learning activities.
• Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

• If staff or pupils discover unsuitable sites, including those promoting radicalised or extremist views, or opinions, then under the new Counter Terrorism and Security Act 2015 schools (and other authorities) are obliged to prevent people from being drawn into terrorism. The URL (address), time, date and content must be reported to the school ICT Leader and Head Teacher.
• Staff must ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
• Pupils will be taught to be critically aware and evaluate the materials they read and be shown how to validate information before accepting its accuracy, such as:

1. Is the website linked to a familiar organisation or brand?
2. Are the links from the website appropriate?
3. Can the information be confirmed on other websites?
4. Is the website trying to encourage people to have different views that cause upset, hatred or even harm?

Managing Internet Access
Information system security

• The security of the school information systems will be reviewed regularly.
• Virus protection will be installed and updated regularly.
• The school uses broadband with its firewall and filters. This system is installed on all laptops and desk tops computers accessed by both children and staff.

E-mail

• Pupils may only use approved e-mail accounts on the school system. **Children are not allowed access to personal e-mail accounts or chat rooms whilst in school.**
• Pupils must immediately tell a teacher if they receive an offensive e-mail.
• Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.

Published content and the school website

• The contact details on the school website should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
• The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

• Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
• Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
• All parents / carers are asked for permission for their children's photograph to be taken and uploaded to the school website. At no point will a photograph be uploaded online with a child's full name.

Social networking and personal publishing

• Social networking sites and newsgroups will be blocked unless a specific use is approved (such as being used as a vehicle for updating parents of school dates and news).
• For pupils who are allowed or access social networking sites out of school, as part of The Henry Princes' PSHE/ Digital Literacy units of work, as with any website accessed by children, they shall be advised never to give out personal details of any kind which may identify them or their location. Examples include real name, address, mobile or landline phone numbers, school, e-mail address, names of friends, specific interests and clubs etc.
• Pupils and parents will be reminded/advised that the use of social network spaces, such as Facebook and Twitter, have an age requirement of thirteen and above, hence they are inappropriate for primary aged pupils. In addition to this, these sites are often open to the public domain and can permit avenues of communication and the exploitation of vulnerable young people and adults to involve them in terrorism or the support of terrorist activity.
• If it is disclosed that children are accessing social media sites and are involved in such activity, whereby they are receiving extremist information or messages, or they are choosing to take part and/or post such content, then this will be reported to the designated Child Protection Officers (Head and Deputy Head Teachers) immediately and reported to the Staffordshire Police Prevent Team.
• Any slanderous comments about the school, staff or other pupils shall be recorded and passed on to Staffordshire Police. The law concerning social media, such as Twitter is clear - if you make a defamatory allegation about someone you can be sued for libel. It is the same as publishing a false and damaging report in a newspaper. Source: http://www.bbc.co.uk/news/magazine-20782257

Mobile phones

• The use of mobile phones is not permitted within school by children. Staff must have their mobile phones turned off during curriculum time. Staff can be contacted via the school office during this time if necessary.
• Those children who choose to bring a mobile phone to school hand them in to the Office where they are kept in a secure place until they are collected at the end of the school day.
• It is strictly prohibited for mobile phones to be used by staff or parents to photograph children both in school and when taking part in out of school visits. This measure is to safeguard both children and adults working with children.

Managing filtering

SEPM has been installed on all school devices. SEPM detects potentially inappropriatecontent, including extremist material, and conduct as soon as it appears on screen, is typed in or receivedby the user. A screen capture is taken of every incident detailing the time and date of capture. A weekly

headline summary is produced from the system detailing captures of particular interest to alert the Head Teacher and ICT Leader immediately, who monitor the system.
• The school will work in partnership with the service provider to ensure filtering systems are as effective as possible.
• If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school Esafety leader using the provided record sheet.
• All extremist materials shall be reported to Staffordshire Police Prevent Team.

How does SEPM protect pupils?

SEPM monitors an ICT network and alerts staff to inappropriate or risky behaviour
Typically captures:
Cyberbullying
Proxy by-pass use
Explicit images
Swearing
ICT misuse

How does SEPM transform behaviour?

Acts as an effective deterrent by setting enforceable boundaries for acceptable use. It empowers schools to encourage appropriate behaviour, keep pupils on-task in lessons, give pupils responsibility for their actions and learn for themselves what is safe.
How will we make children/staff/parents aware that it is in place?
School Assembly, staff briefing, information letter to parents

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.
Staff users will be made aware of the filtering systems through:
• signing the AUA
• induction training
• staff meetings, briefings, Inset.
Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through e-safety awareness sessions / newsletter etc.

Protecting personal data

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

Written: September 2016

Signed: _____ Dated:_____

Staff Acceptable Use Agreement (SAUA)

✓ I will only access the system with the login and password that I have been given and will not access other people's files without permission
✓ I will only use appropriate software, computer media and websites when working alone or with children.
✓ I will not download software or files.
✓ I will not give out personal information or information about children.
✓ I will report any unpleasant material or messages I find, are sent to me, found by children or sent to children
in my care, including messages of radicalised views and/or content (particularly through social media).
✓ I will endeavour to maintain the security of any files stored on laptops or portable media when taking these
out of school.
✓ I understand that there will be checks and monitoring of computer use and the internet sites that I visit.
✓ I understand that any reports will be confidential and will help protect myself and other users.
✓ I understand that it is not recommended that school computers are used for personal reasons. However, if I do use the school computers for personal reasons I must do so responsibly and understand that this will be monitored.
✓ I understand that it is against my contractual obligations to have online contact with current or previous pupils.
✓ I understand that social networking should not be used as a medium in which to discuss any matters regarding my professional life or school business. I also understand that anything that I may post online to my friends, family, colleagues or acquaintances, may be viewed by other contacts, including statements and opinions I post or pictures, including photographs, that are linked to me or my accounts. In addition to this, my current employer, or employers in the future may search for my name on the Internet. For example, social media.

I agree to abide by this agreement

Name: _____

Signature: _____ Date: _____