



HIGH MEADOW INFANT SCHOOL

E SAFETY POLICY

2018 - 2019

Date for review - Autumn Term 2019

Introduction

Our E-Safety Policy has been written by the school, building on the Warwickshire ICT Development Service E-Safety Policy and government guidance. It has been agreed and approved by Governors.

The E-Safety Policy will be reviewed annually or as new technologies emerge. There is a "whole school ownership" of the policy. It has been developed in consultation with a wide range of staff.

The E-Safety Policy covers the use of all ICT systems, equipment and software in school, including the internet, email, computers, laptops, tablets, cameras, mobile phones and other mobile technologies.

It also addresses school related ICT out of school and the use of personal ICT equipment in school.

The school is committed to act on E-Safety incidents both inside and outside the school on issues that will affect the well being of staff and pupils.

Incidents raising concerns about the safety of any children will be dealt with in accordance with the Safeguarding policy.

Staff development in safe and responsible internet use, information security and the school E Safety Policy will be provided as required.

Teaching and Learning

The Internet is an essential element in 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.

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 information and business administration systems.

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries
- 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 the LA and DfES
- Access to learning wherever and whenever convenient e.g. through the Warwickshire Learning Platform

How will pupils learn how to evaluate Internet content?

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. 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 Warwickshire LA can accept liability for the material accessed, or any consequences of internet access. Therefore pupils need to have input on how to evaluate information received. They also need to be taught what to do in case they are confronted with something distasteful/unsuitable.

Evaluation also needs to be made regarding the accuracy of the information they are looking at. Pupils will be taught in E-Safety lessons and throughout other lessons to question the source of Internet information and its reliability.

Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

Pupils should be taught research techniques and key information handling skills and the evaluation of on-line materials is a part of every subject.

If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to Warwickshire ICT Services.

Managing Information Services

The security of the school information systems will be reviewed regularly through the use of Warwickshire Broadband with its firewall and filters (Smoothwall).

The school provides an additional level of protection through its deployment of Policy Central in partnership with Warwickshire ICT Development Service.

We recognise that Information Management is a complex and multi-faceted set of processes. Information/ data held is a major responsibility which can have implications for the personal safety of staff and pupils. 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.

Therefore, security strategies will follow Warwickshire LA guidelines. The security of the school information systems will be reviewed regularly and virus protection will be updated regularly.

This will be managed by the half termly visits from the Warwickshire ICT co-ordinator.

Personal data sent over the Internet will be encrypted or otherwise secured.

Staff will not use their personal email for school business. This is especially important when considering files with data as Warwickshire holds the messages and not external email agencies.

Protecting Personal Data

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

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.

Passwords/Security

All staff have individual logins and passwords to ensure personal accountability and security. All staff know to keep passwords secret. All staff will be aware of a login for computers children will access.

How will email be managed?

To ensure safety, pupils may only use Warwickshire approved e-mail accounts (username@welearn365.com which is monitored) on the school system and will adhere to our acceptable use agreement.

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.

When using email to contact external organisations these should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Video Conferencing (including internet telephony such as Adobe Connect)

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.

When considering the equipment and network, this will be maintained by the LA ICT Technician. As a school, we will ensure that all video conferencing equipment in school is switched off when not in use and not set to auto answer.

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.

When considering its use, unique log on and password details for video conferencing services should only be issued to members of staff and kept secure. Video conferencing should be supervised at all times. Pupils should ask permission from the supervising teacher before making or answering a video conference call.

When considering its content, Video conferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.

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 video conference 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).

It is important to establish dialogue with other conference participants before taking part in a video conference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class.

How will published content be managed?

The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.

Photographs and video images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by their full name.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Staff will take full responsibility in deleting class photos on computers, tablets, cameras and other ICT equipment at the end of the three years that the child attends the school.

Staff will not take school cameras home. Staff will not take photos of children on their own personal devices. (e.g. phones and cameras)

How will social networking and personal publishing be managed?

All users will sign the Acceptable Use Agreement / E Safety Rules.

Pupils will use the Warwickshire 365 Learning Platform as a safe way of emailing/video messaging/blogging/discussing.

Video conferencing is only to be used with a member of staff leading. Pupils will not be left unattended whilst using these technologies.

Written permission from parents/carers is needed before images (pictures and videos) of pupils are used.

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, email address, names of friends etc.

How will filtering be managed?

The school will work in partnership with the Warwickshire ICT Development Service to ensure filtering systems are as effective as possible.

If staff or pupils discover unsuitable sites, Warwickshire ICT Development Service will contact the school and inform the head teacher.

In addition, staff will contact the Warwickshire ICT Development Service and inform them of any unsuitable sites that need to be blocked.

How can emerging technologies be managed?

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

Personal mobile phones/hand held devices will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden. Staff keep their mobile phones in their locked locker in the staff toilets during school time. Staff can check for messages during their breaks but are not allowed to take them past the school hall doors unless with permission from the head teacher.

How should personal data be protected?

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

Policy Decisions

How will internet access be authorised?

The school will keep a copy of all staff and pupils who are granted Internet access. All users have individual passwords to access the computers and laptops. Each class uses a class user and password.

All users must read and abide by the 'Acceptable Use Agreement' before using any school ICT resource.

Parents will be asked to read and acknowledge the school's 'Acceptable Use Agreement'.

How will risks be assessed?

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. 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 WCC can accept liability for the material accessed, or any consequences of Internet access.

If staff or pupils discover unsuitable sites, Warwickshire ICT Development Service will contact the school and inform the head teacher. In addition, staff will contact Warwickshire ICT Development Service and inform them of any unsuitable sites that need to be blocked.

All users must read and abide by the Acceptable Use Agreement which also asks that E-Safety rules be implemented in school and at home.

Pupils are educated about the risks of internet misuse through regular PHSE lessons and e-safety lessons. E-safety will be taught as a half-term unit in KS1 in addition to all classes taking part in E-Safety day.

All children will be introduced to 'Hector the Protector' and encouraged to click on him to cover the screen if anything happens online that they are unsure about.

Staff are aware that there may be unannounced spot checks on staff laptops.

Cyber Bullying

Pupils in the school have Internet Safety lessons which discuss potential issues, including cyber bullying.

Cyber Bullying is listed as unacceptable behaviour in the school's Behaviour Policy.

The culture of the school encourages all members to report any misuse of ICT, including internet misuse. Pupils are encouraged to inform a member of staff if worried about any aspect of internet misuse or other ICT issues.

How will e-safety complaints be handled?

All E-Safety incidents will be logged on an orange E Safety Incident form and handed to the DSL or deputy DSL. Together, it will be agreed what course of action will be taken.

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. Any complaints referring to the Head Teacher must be referred to the Chair of Governors.

Sanctions

All pupils and staff are aware of the responsibilities they have when using the internet at school and home.

Teachers should refer to the Teachers' Standards documentation in respect of their professional conduct and behaviours. (Appendix C - Teachers Standards - Part 2) within and outside school.

Pupils will be reminded of e-safety procedures every half term as part of the computing curriculum. Pupils in KS1 will also be taught an e-safety unit.

How is the internet used across the community?

The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

Communications

How will the policy be introduced to pupils?

All pupils must read and abide by the Acceptable Use Agreement.

Rules for Internet access (SAFE) will be posted in all networked rooms.

Pupils will be informed that Internet use will be monitored.

An E-Safety training programme will raise the awareness and importance of safe and responsible Internet use. Internet Safety week will be used each academic year and an E Safety parents workshop will be offered every academic year.

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

How will policy be discussed with staff?

All staff will be given the School E-Safety Policy and its importance explained, including the induction of new staff.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Staff should also be aware that laptops may be spot checked and that internet access at home on the school laptop is still monitored. Discretion and professional conduct is essential.

All users must read and abide by the Acceptable Use Agreement. In addition, staff must read and abide by the Warwickshire School Acceptable Use Policy.

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 E-Safety Policy will be provided as required.

How will parents support be enlisted?

Parents' attention will be drawn to the School E-Safety Policy in newsletters and on the school website.

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

A partnership approach with parents will be encouraged. This will include parents' workshops with demonstrations and suggestions for safe home Internet use.

A 'Surfing Safely' booklet will be available on the school website and there are E Safety links at the bottom of every weekly school newsletter.

Signed and Agreed - December 2018.

Head Teacher Mrs D Y Hughes ICT Co-ordinator Miss L Edwards