Hoole St. Michael’s Church of England Primary School

Online Safety Policy

Member of staff responsible: J Price
Date policy written: February 2018
Date approved by the Standards and Effectiveness Committee: February 2018
Date for next review: February 2020

Mission Statement

Christ’s love is in everything we do at Hoole St Michael. Our creative and high-attaining Church of England Primary School is safe, loving and supportive. We encourage the building of good relationships and friendship through respect, tolerance and understanding. Within our Christian family, where parents are our partners in all aspects of school life, we aim to inspire a love for learning within each and every child.

Contents

1. Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective eSafety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our eSafety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings. The policy is organised in 4 main sections:

- Policies and Practices
- Infrastructure and Technology
- Education and Training
- Standards and Inspection

2. Hoole St. Michael's vision for eSafety

At Hoole St Michael we use technology, when appropriate, to enhance and support the learning experience for our children and to aid the daily organisation and administration tasks carried out by school staff. Keeping members of our school and community safe, whilst using technology is a responsibility and we expect staff to act as role models in their use of technology, abiding by the shared decision reflected in our eSafety policy. Children are encouraged to explore, recognise risks and make responsible decisions regarding their use of technology and we will provide opportunities for the children, staff, parents and the wider community to understand and view eSafety education as a key life skill. We will ensure children are aware of ways to deal with risks both in and out of the school environment. Our eSafety policy defines what we consider to be acceptable and unacceptable behaviour regarding the use of technology in school and the procedures to be followed should breaches of security occur. This policy will be shared with staff, governors, parents and pupils and will be updated when necessary with the introduction of new technologies or incidents.

3. The role of the school's eSafety Champion

Our eSafety Champion is Mrs J Price-Headteacher (with the assistance of Mrs S Cookson-Deputy Headteacher. Mr N Woodcock-Chair of Governors)

The role of the eSafety Champion in our school includes:

- Having responsibility for ensuring the development, maintenance and review of the school's eSafety and Acceptable Use Policy (AUP) policy.
- Ensuring that the policy is implemented and that compliance to the policy is monitored.
- Ensuring all staff are aware of the reporting procedures and requirements should an eSafety incident occur.
- Ensuring the eSafety Incident Log is appropriately maintained and regularly reviewed.
- Keeping up-to-date with the eSafety issues and guidance through liaison with the Local Authority Schools' ICT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging eSafety advice/training for staff, parents/carers and governors.
- Ensuring all staff, pupils and governors are updated as necessary.

- Liaising with the school's Designated Senior Person (DSP) to ensure a co-ordinated approach across relevant safeguarding areas.

4. Policies and practices

This section of the eSafety policy sets out our approach to eSafety along with the various procedures to be followed in the event of an incident.

4.1 Security and data management

In our school data is kept secure and all staff are informed what they can/cannot do with regard to data in the following ways:

- Key information/data is mapped and securely stored on the main office and headteacher office computers. This is only accessible by the bursar and headteacher.
- The headteacher has overall responsibility for managing all information.
- Staff have been informed of the location of all data relevant to them by the headteacher.
- Staff have been informed of their legal responsibilities in line with the requirements of the Data Protection Act (1998) and ensure all data is:
    1. Accurate
    2. Secure
    3. Fairly and lawfully processed
    4. Processed for limited purposes
    5. Processed in accordance with the data subject's rights
    6. Adequate, relevant and not excessive
    7. Kept no longer than necessary
    8. Only transferred to others with adequate protection

Our school ensures that data is kept appropriately and managed both within and outside the school in the following ways:

- School's equipment, including teacher laptops, must only be used for school purposes and do not contain personal information e.g. personal images, personal financial details, music downloads, personal software. Computers are also accessed using a safe username and password and it is the responsibility of each individual to keep this secure at all times. Any breaches in security must be reported immediately to Mrs J Price
- School equipment must not be used, for online gambling, dating websites, home shopping, holiday booking, and social networking **both in school and at home.**
- Staff are aware of the school's procedures for disposing of sensitive data, such as shredding hard copies, deleting digital information, deleting usernames and passwords from school's VLE, deleting email accounts, TLPs and SATs information and know the persona should there be any queries.
- School has purchased a 'back-up' shredder to ensure there is always availability for safe disposal of documents. Each staff member is responsible for the disposal of documents securely. Main shredder in school office; back-up shredder in HT office.
- Remote access to the Headteachers School desktop, only they will be allowed to access data from home via a secure wireless connection. School data MUST NOT be stored on personal equipment.
- Staff are not allowed to use personal storage devices e.g. external harddrives, pendrives or mobile phones on school equipment.

- Each teacher has been provided with an encrypted, password protected device to use on school equipment when necessary to store data as part of their professional role such as, writing IEPs, writing reports or backing up reports.

4.2 Use of mobile devices

- Staff at Hoole St Michael have been provided with lockers to ensure the secure storage of valuables such as mobile phones whist at work.
- The use of mobile phones is not permitted in any area where there are children and staff are not permitted to have their phone on their person at any time.
- Mobile phones are only to be used in the bursar's office, head's office and in the staffroom.
- Children who bring a phone to school when necessary for safety e.g. walking home alone; will store the device in the office which is locked securely all day. The children will hand the phone in at the start of the day and collect at the end of the day. For more detail please see the school's mobile phone policy.

4.3 Use of digital media

- In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below.
- All users of digital media (photographs, video) in our school are informed and educated about the risks surrounding taking, using, sharing, publishing and distributing digital media.
- Parental permission is always obtained before images are used in school brochures or published on the school website.
- Generic parental/care consent to use children's images within the school is obtained on a regular basis and kept securely in the school bursar's office.
- Full names and personal details are never used on any digital media.
- Parents/carers using digital media to record images at school events are always cautioned not to publish any on Social Networking sites or to circulate images.
- All staff are aware that personal equipment must not be used to store digital content.

4.4 Communication technologies

Email:

In our school the following statements reflect our practice in the use of email.

- All users in our school have access to Office 365 as the preferred school email system. This system came into place in the autumn term 2014.
- Only official email addresses are used to contact staff or pupils.
- All users are aware that email is covered by the Data Protection Act (1998) and the Freedom of Information Act (2000), meaning that safe practice follows in respect of record keeping and security.
- All users are aware that email content may be monitored at any time in accordance with the Acceptable Use Policy.
- All users must immediately report any mail that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
- All users are encouraged to use the following disclaimer at the bottom of all outgoing emails (see next page)

Example of email disclaimer:
This email and any files transmitted within it may be confidential and are intended solely for the individual to whom it is addressed. Any views or opinions presented are those of the author and do not represent Hoole St Michael Primary School. If you are not the intended recipient, you must not use, disseminate, forward, copy or print this email or its contents. If you have received this email in error, please contact the sender. Please note that email may be monitored in accordance with both school policy and the Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000.

Social Networks:
In our school the following statements outline what we consider to be acceptable and unacceptable use of Social Network sites outside of school:
As part of the Acceptable Use Policy, all staff sign up to the following rules:

- There will be NO access to Social Networking sites except on the HT's computer to update the school's Twitter feed.
- Adults are not allowed to communicate with pupils using and digital technology where the content of the communications may be inappropriate or misinterpreted.
- Adults in school are NOT permitted to add pupils or past pupils as 'friends' on Social Networking sites.
- Children are given guidance on the age restrictions of certain Social Networking sites and educated about the need to keep themselves e-safe.
- Many adults and pupils regularly use Social Network sites, e.g.Club Penguin, Moshi Monsters, Facebook or Twitter, although the minimum age for registering for some of these excludes primary school pupils. These communication tools are, by default, 'blocked' through the internet filtering system for direct use in Lancashire schools. However, comments made outside school on these sites may contravene confidentiality or bring the school or staff into disrepute.

Instant Messaging:
In our school the following statements outline what we consider to be acceptable and unacceptable use of Instant Messaging:

Web sites and other online publications:
Our school website is maintained and administered by the headteacher and each class teacher has access for the purpose of sharing information with parents about each individual class or to share work; the chair of the PTFA and Manager of Kids' Club have access to their pages only on the school website. A governor, Mr Neil Kenyon also has access to the school website to support the HT in its maintenance. Weekly newsletters, key policies, key events and information are advertised and displayed on the school website. The general public can only visit the designated class areas and the public areas of the school website. All staff are aware of the guidance regarding digital media and children's details.

Video conferencing:
If and when video conferencing should take place the headteacher gives approval before the session. Permission letters are sent out to parents/carers to ensure each child has written permission. Children who do not have consent are withdrawn from classrooms when video conferencing is in progress. All staff are aware of copyright, privacy and Intellectual Property Rights legislation.

Others:
Currently, the school does not use Bluetooth or Infrared communication technology.

4.5 Acceptable Use Policy (AUP)

An AUP is intended to ensure that all users of technology within school will be responsible and stay safe. It will help ensure that all users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes. All staff sign and abide by an Acceptable Use Policy which protects the school, pupils and themselves from potential risk.
All children also sign and abide by an Acceptable Use Policy to protect their interests.
All parents and carers sign an Acceptable Use Policy to protect the children outside the school.
Rules regarding the acceptable use of technology are displayed in all classes.
Children, staff and parents/carers are regularly reminded of the sanctions in place in case of breach of the rules for the acceptable use of technology in school.

4.6 Dealing with incidents

As a staff we have considered the incidents that may occur in school and have agreed a plan of action that each member of staff will follow.
eSafety infringements of a minor nature are dealt with by members of staff in the classroom.
A major breach of the rules has to be reported to the eSafety champion, the Headteacher and logged in the eSafety incident log which is situated in the headteacher's office.

5. Infrastructure and technology

- Our school subscribes to the Lancashire Grid for Learning/CLEO Broadband Service where internet content filtering is provided by default. The filtering service provides a high level of protection, but all staff members are made aware of eSafety issues and children may not access potentially harmful sites (like Google images or games sites) without adult consent.
- Sophos Antivirus software is installed on all computers that access the school server.

Pupil Access:

- Children are always supervised when using technology in school.
- Children must seek adult supervision before accessing online materials.
- All staff will check any website they direct the children to for an independent task before the lesson to ensure all content and links the website may take you to are acceptable.

Passwords:

- All staff are aware of the guidelines in the Lancashire ICT Security Framework for Schools (www.lancsngfl.ac.uk/esafety)

- All users of the school network have secure usernames and passwords.
- The administrator password for the school network is only available to the ICT technician and the eSafety champion and is kept safe by the eSafety champion.
- All staff and pupils are regularly reminded to keep passwords secure.
- Passwords for school systems are created by individuals and known only to individuals concerned.

Software/hardware:

- The school have legal ownership of all software.
- Software licences are kept in the school bursar's office.
- Equipment is regularly audited and records are kept in the school bursar's office.
- Software installation is only carried out by the school ICT technician who is monitored by senior members of staff.

Managing the network and technical support:

- All servers, wireless systems and cabling are securely located and physical access is restricted.
- All wireless devices are security enabled.
- All wireless devices are only accessible through a secure password known only to the school ICT technician.
- Security for the school network is provided by the Lancashire School's ICT centre and our designated school ICT technician, currently Mr Rory Woodward
- Safety and security of our school network is reviewed regularly by the school ICT technician.
- School systems are kept up to date and updated with critical software updates/patches on a regular basis by the school ICT technician who visits the school 3 x per week.
- All users (staff, pupils, guests) have clearly defined access rights to the school network. Staff and pupils each have their own designated password to access the school network; guests (such as supply teachers) are allocated temporary access via a temporary password.
- Staff and pupils are required to log out of a school system when a computer/digital device is left unattended.
- No users are allowed to install executable files or install software – this is only done by the school's ICT technician during his weekly visits.
- Users report any suspicion or evidence of breaches of security to the eSafety champion and the school ICT technician who attends to it.
- Each teacher has a designated laptop for use for planning purposes.
- Staff are aware that teacher laptops are school property and that they must not be used to store or download excessive or inappropriate content of a private nature.
- All internal/external technical support providers are aware of our school's requirements and standards regarding eSafety.
- The school computer subject leader (currently Mrs Louise Horn) and also the school eSafety champion are responsible for liaising and managing technical support staff.

6. Education and Training

Education and training are essential components of effective eSafety provision. It is important to equip individuals, particularly pupils, with the appropriate skills and abilities to recognise the risks and teach them effective ways to deal with them is fundamental. eSafety guidance must be embedded within the curriculum and advantage taken of new opportunities to promote eSafety. This section of the policy outlines how eSafety messages are communicated to the various stakeholder groups in our school community.

6.1e Safety across the curriculum

We provide regular eSafety teaching to staff and pupils via our computing curriculum. *There is an additional focus on eSafety during 'Safer Internet Day' and during Anti-Bullying Week. Children are made aware of how to keep themselves eSafe. Pupils are taught about Data Protection and Copyright Legislation. Pupils are taught to critically evaluate materials and develop good research skills. eSafety rules are displayed in classrooms and designated areas to keep children safe.*

6.2e Safety – Raising staff awareness

All staff are regularly updated on eSafety via staff meetings. The schools eSafety Champion provides guidance and training as when required.

6.3e Safety – Raising parents/carers awareness

Parents/carers are regularly updated about eSafety via the weekly school newsletter and annually via the Acceptable Use Policy for Parents and Carers and eSafety workshop.

6.4e Safety – Raising Governors' awareness

Governors are regularly updated about eSafety via the weekly school newsletters and annually via the school's eSafety Policy. They are also invited to attend LCC Governor Training

7 Standards and inspection

The effectiveness of our eSafety Policy is monitored by the eSafety champion, computing subject leader and every member of staff in our school. Any incidents are recorded and analysed to ensure any issues do not become a greater issue.

Any new technologies are risk-assessed before installation by the school ICT technician and monitored by members of staff.

Developing and Reviewing this Policy

This eSafety Policy has been written as part of a consultation process with staff and governors

It has been approved by Governors and will be monitored and reviewed annually at the spring term Standards and resources ' governor sub-committee.

Signed ____ Headteacher

Signed ____ Chair of Health and Safety