Hollinswood Primary School & Nursery

Online Safety Policy

December 2022

Document Status -	
Policy Authors	Hollinswood Primary School & Nursery
Policy Created Date	
Policy Previous Review Date	May 2019
Current Policy Date	11th December 2022
Policy Review Frequency	Annually
Date of Next Review	January 2024
Committee/Approver of Policy	Full Governors

Introduction

The Online Safety Policy is part of the School Development Plan and relates to other policies including Acceptable Use Policies for Staff and Students, Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy and Social Media Policy.
The school's Computing Coordinator will also act as Online Safety Coordinator.

Our Online Safety Policy builds on government guidance and has been agreed by senior management and approved by governors. The Online Safety Policy and its implementation will be reviewed annually.

Background/Rationale

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Our school online safety policy helps to ensure safe and appropriate use. The development and implementation of such a strategy involves all the stakeholders from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students / pupils themselves.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / online games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and this online safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school has provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. The online safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

It is our responsibility

1. To protect and educate pupils and staff in their use of technology
2. To have the appropriate mechanisms to intervene and support any incident where appropriate in these four areas of risk:

a. Content: being exposed to illegal, inappropriate or harmful material
b. Contact: being subjected to harmful online interaction with other users
c. Conduct: personal online behaviour that increases the likelihood of, or causes, harm
d. Contract/Commerce: potentially being exploited by commercial interests (gambling)

Our online safety risk assessment details how we minimise risk against the 4C's. See appendices.

Other actions we take:

1. Provide annual staff training to improve knowledge of and expertise in the safe and appropriate use of new technologies
2. To work closely with all families to help them ensure that their children use new technologies safely and responsibly both at home and at school - advice in newsletters, online safety presentation for parents, updates via ClassDojo as and when appropriate, communicating with parents via twitter and the school website, giving advice and support to parents/carers when needed on a 1:1 basis.
3. To use pupils' and families' views more often to develop online safety strategies.
4. To help pupils understand how to manage risk; to provide them with richer learning experiences; and to bridge the gap between systems at school and the more open systems outside school through Computing and PSHE lessons.
5. To provide an age - related, comprehensive curriculum for online safety that enables pupils to become safe and responsible users of new technologies.
6. To systematically review and develop online safety procedures, including training, to ensure that they have a positive impact on pupils' knowledge and understanding.
7. To deliver half-termly up-to-date and relevant online safety challenges across the whole school, researched and set by the Online Safety Coordinator. These challenges, set to ensure all the pupils at school understand how to stay safe on the internet, are completed during Computing curriculum time, ensuring that teaching staff have time to deliver the lesson.

We update staff and students (as appropriate based on age) of developments in the <u>four areas of risk</u>

1. Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- Lifestyle websites, for example pro - anorexia/self-harm/suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content

2. Contact

- Grooming, stalking
- Cyber - bullying in all forms
- Identity theft and sharing passwords

3. Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well - being (amount of time spent online (internet or gaming))
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images)
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)

4. **Contract/Commerce**
   Children being party to and/or exploited by a potentially harmful contract/commerce or commercial interests, including:
   - Gambling
   - Exploitative or Age-Inappropriate marketing
   - Identity theft
   - Fraud
   - Scams
   - Trafficking
   - Streaming Child Sexual Abuse

Whole School Consistent Approach:

All teaching and non-teaching staff can recognise and are aware of online safety issues. High quality leadership and management make online safety a priority across all areas of the school.

A high priority is given to training in online safety, extending expertise widely and building internal capacity.
The contribution of pupils, parents and the wider school community is valued and integrated.

Pupils' Access to the Internet

At school we use Telford & Wrekin Council's actively monitored and filtered Internet Service, which will minimise the chances of pupils encountering undesirable material. No pupil is able to use a mobile phone during school hours/trips and so internet access should only occur via the school networks. Members of staff will be aware of the potential for misuse, and will be responsible for explaining to pupils, on a regular basis, the expectation we have of them. Teachers will have access to pupils' emails and Office365 accounts, and will make periodic checks these on a regular basis to ensure expectations of behaviour are being met.

Senso software runs on the school network and monitors the computer usage of pupils and staff. Inappropriate words or phrases are flagged up via the software, which is monitored regularly by senior leadership.

Expectations for Internet Use

- We expect everyone to be responsible for their own behaviour on the Internet, just as they are anywhere else in school.
- Pupils must always ask permission before using the Internet and have a clear idea why they are using it.
- Children and staff will never reveal personal details, home addresses and telephone numbers on the web or in dialogue with other Internet users.
- Children are only permitted to use school accounts for email. All email will be moderated and monitored by the class teacher. The use of unfiltered web-based email is not permitted.
- Children will not engage in any form of conversation or dialogue with other users on the Internet without permission and supervision from their teacher.
- The use of public chat rooms and Internet Messaging Services is prohibited.
- The use of social networking sites such as Instagram or Facebook are not generally appropriate to education and the use of the Internet for such purposes is not permitted.
- Computers should only be used for schoolwork and homework.
- Files may only be downloaded by staff, or children under supervision.
- Pupils using the Internet are expected not to deliberately seek out offensive materials. Should any such material be encountered accidentally, or if any child finds themselves uncomfortable or upset by anything they discover on the Internet, they will turn off the monitor immediately and report it immediately to the supervising adult. (Any adult should report it to the Head Teacher immediately. Arrangements can then be

made to request that Telford & Wrekin Council blocks the site). Children are taught these flagging arrangements from KS1.
- Pupils should generally only access the network using their own personal login. No network user should access other people's files unless permission has been given.
- Online Safety rules are shared by class teachers at the start of each academic year and displayed as a reminder in the classroom. See appendices

Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school:

1. Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports.

2. Headteacher and Senior Leaders

- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community.
- The Headteacher and Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

3. Online Safety Coordinator

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with T&W ICT technical staff

4. Technical Staff

The Local Authority and ICT Technician are responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- That the school meets the online safety technical requirements outlined in any relevant Local Authority Online Safety Policy and guidance
- That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- That he / she keeps up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the network / remote access / email is regularly monitored via Senso in order that any misuse / attempted misuse can be reported to the Online Safety Co-ordinator
- That monitoring software / systems are implemented and updated as agreed in school policies

5. Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Policy (AUP)

- They report any suspected misuse or problem to the Online Safety Co-ordinator or other member of the Senior Leadership Team
- Digital communications with students / pupils (email / voice) should be on a professional level *and only carried out using official school systems*
- Online safety issues are embedded in all aspects of the curriculum and other school activities
- Pupils understand and follow the school online safety and acceptable use policy
- They monitor ICT activity in lessons, extra curricular and extended school activities
- They are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

6. Designated Person for Child Protection

Should be trained in online safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

7. Pupils

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy (online safety rules)
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school (as mentioned in the online safety rules).

8. Parents/Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through ***parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature.***

Parents and carers will be responsible for:

- Endorsing the Pupil Acceptable Use Policy (shared when pupils join the school)
- Accessing information on ClassDojo or the school website regarding online safety

9. Community Users

Community users who access school ICT systems / website as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

Technical - Infrastructure

- The school will be responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.
- School ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined any relevant Local Authority Online Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded and reviewed, at least annually.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by T&W
- Any filtering issues should be reported immediately to T&W
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Senso remote management tool is used by staff to control workstations and view users' activity
- An appropriate system is in place for users to report any actual / potential online safety incident – pupils are asked to report to their class teacher or teaching assistant and staff should report to a member of the Senior Management Team, who will then refer to the Headteacher.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- Provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system can be permitted through a temporary log on / email granted through T&W. Users must sign the AUP before this can take place.
- The school infrastructure and individual workstations are protected by up to date virus software.

Education

1. **Pupils**

   Whilst regulation and technical solutions are very important, their use must be balanced by educating *pupils* to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. This will be done in the following ways:

   - A planned online safety programme should be provided as part of Computing / PHSE curriculum and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. This is covered through the Digital Literacy strand of the Computing curriculum in detail each Autumn term and is revisited by half termly online safety challenges throughout the year.
   - Key online safety messages should be reinforced as part of a planned programme of assemblies and themed days throughout the school year e.g. Safer Internet Day.
   - Pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information. Pupils will be informed that internet use may be monitored.
   - In lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. Safe

searching is covered in the computing curriculum and use of child friendly search engines (eg Kiddle) is encouraged.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Staff should act as good role models in their use of ICT, the internet and mobile devices

2. Parents and Carers

Some parents and carers have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring of children's online experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report). Therefore, parents' attention will be drawn to the School Online Safety Policy in newsletters, ClassDojo and on the school website on a regular basis.

3. **Staff**

It is essential that all staff receive annual online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Annual online safety training will be made available to all staff. An audit of the online safety training needs of all staff will be carried out regularly. It is expected that some staff may identify online safety as a training need within the performance management process.
- All staff will be given the School Online Safety Policy and its importance explained.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policies
- The Online Safety Co-ordinator will attend training sessions and review guidance documents released by LA and other relevant sources.

4. **Governors**

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in ICT / online safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association or other relevant organisation
- Participation in school training / information sessions

Content

Use of digital and video images – photographic, video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

Published content and the school web site
The contact details on the website should be the school address, email 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. This is part of the school admissions form.

Pupils' work can only be published with the permission of the pupil and parents. This is obtained when children join the school.

Social networking and personal publishing
- The school will block/filter access to social networking sites e.g. Facebook
- Newsgroups will be blocked unless a specific use is approved. Pupils will be advised never to give out personal details of any kind that may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Protecting Personal Data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. This states that data should be:
1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate
5. Kept no longer than is necessary
6. Processed in accordance with the data subject's rights
7. Secure
8. Only transferred to others with adequate protection.

Staff must ensure that they:
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

- Transfer data using encryption and secure password protected devices.
- Personal data must not be stored on any portable computer system, USB stick or any other removable media.

School website/twitter guidelines
A website can celebrate good work, promote the school, publish resources for projects and homework, and link to other good sites of interest. However, to protect our children, the following guidelines will be adhered to:

- Children are only referred to by first names on our school website
- Individual images of children will not be used unless permission is granted from parents
- Group photographs will not contain a names list
- We will only use images of pupils in suitable dress
- Home information and email identities will not be included - only the point of contact to the school, i.e., telephone number, school address and email to the school office
- Work displayed will be of the highest quality and reflect the status and ethos of the school

Parents who would prefer that their children do not appear on our school website, for whatever reason, are asked to inform the school. An up-to-date list of such children is kept in the school staff room and referred to before new pages are added. If, at any time, a parent expresses concern about usage of an image or piece of work, it will be removed from our site as quickly as possible.

Assessing Risks
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 LA can accept liability for the material accessed, or any consequences of Internet access.

It is most likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through the school behaviour policy. However, if a pupil is deliberately accessing or trying to access material that could be considered illegal, police advice should be sought.

Handling Online Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.