HOLDEN LANE
PRIMARY SCHOOL

Online Safety Policy

September 2022-2024

ONLINE SAFETY POLICY

Online Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The ‘staying safe’ outcome of the Every Child Matters Agenda includes aims that children and young people are:

- Safe from maltreatment, neglect, violence and sexual exploitation
- Safe from accidental injury and death
- Safe from bullying and discrimination
- Safe from crime and anti-social behaviour
- Secure, stable and cared for

Many of these aims apply equally to the ‘virtual world’ that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the Internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of our school to ensure that every child in our care is safe, and the same principles apply to the ‘virtual’ world as applies to our academy’s physical buildings.
This policy document is drawn up to protect all parties – the students, the staff and the school aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

This policy will operate in conjunction with other policies including those for ICT, Bullying, Curriculum, Child Protection, Data Protection and Security and will be reviewed annually.

Roles and Responsibilities
Online Safety is recognised as an essential aspect of strategic leadership in this school and the Head aims to embed safe practices into the culture of the school.

The Headteacher ensures that the Policy is implemented and compliance with the policy monitored. The responsibility for Online Safety has been designated to a member of the teaching team.

Tracy Bould, our Online Safety Leader, ensures they keep up to date with Online Safety issues and guidance through liaison with the Local Authority. The Online Safety Leader ensures the Headteacher and senior management are updated as necessary.

Trustees need to have an overview understanding of Online Safety issues and strategies at Holden Lane Primary. We ensure that our governors are aware of our local and national guidance on Online Safety and are updated at least annually on policy developments.

Internet Access Holden Lane Primary

The Internet is an essential element in 21st century life for education, business and social interaction. Holden Lane Primary 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.

Teachers and pupils have access to web sites world-wide, offering educational resources, news and current events. There are opportunities for discussion with experts in many fields and opportunities to communicate and exchange information with students and others world-wide.

In addition, staff have the opportunity to access educational materials and good curriculum practice, to communicate with the advisory and support services, professional associations and colleagues; exchange curriculum and administration data with the LA etc; receive up-to-date information and participate in government initiatives.

The Internet is also used to enhance the school's management information and business administration systems.

All staff (including teachers, supply staff and classroom assistants) and any other adults involved in supervising children accessing the Internet, are provided with the Online Safety Policy, and have its importance explained to them. All staff must read and sign the Staff Code of Conduct. All staff will be informed that all computer and Internet use will be monitored and digital cameras are not to be used for personal use. Discretion and professional conduct is essential. Staff will be advised that the use of social networking sites or mobile phones to communicate with pupils and parents is inappropriate.

Ensuring Internet Access is Appropriate and Safe

The Internet is freely available to any person wishing to send e-mail, write a blog, or publish a web site (including social networking sites). In common with other media such as magazines, books and video, some material available on the Internet is unsuitable for pupils. Pupils in school are unlikely to see inappropriate content in books due to selection by publisher and teacher and the school will take every practical measure to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the Internet.

The following key measures have been adopted to help ensure that our pupils are not exposed to unsuitable material:

- Our Internet access is purchased from RM, through Stoke-on-Trent LA, which provides a service designed for pupils including an up-to-date 'firewall' filtering system intended to prevent access to material inappropriate for children including: social networking sites, eBay, YouTube, chat/news/discussion rooms etc.

- Forensic Text Monitoring Software is installed on the school network system. This is intended to proactively encourage appropriate use and act as a deterrent. It constantly monitors **all** communication through the network and provides evidence of misuse, bullying etc. Pupils will be informed that network and Internet use will be monitored.

- Children are taught how to be safe online throughout school. In Year 1, Year 2 and Year 3 pupils are taught to use E-mail and the Internet responsibly in order to reduce the risk to themselves and others. During Year 3, Year 4, Year 5 and Year 6 this safety education is extended to social networking, texting and cyber bullying etc., with appropriate opportunities to discuss, role play and learn about the benefits and risks offered by these new technologies.

- Children using the Internet are supervised by an adult at all times.

- Staff check that the sites pre-selected for pupil use are appropriate to the age and maturity of pupils.

- Staff are particularly vigilant when pupils are undertaking their own search and check that the children are following the agreed search plan.

- Our rules for responsible Internet use are discussed with pupils at the start of each year and as the need arises.

- The Online Safety Leader monitors the effectiveness of Internet access strategies.

- The Head teacher ensures that the policy is implemented effectively.

- Methods to quantify and minimise the risk of pupils being exposed to inappropriate material will be regularly reviewed in consultation with colleagues from other schools and advice from the LA and RM as our internet provider.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Over the past few years, experience has shown that the above measures have been highly effective. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that the particular types of material will never appear on a computer screen. Neither the school nor Stoke-on-Trent City Council can accept liability for the material accessed, or any consequences thereof.

Different ways of accessing information from the Internet are used depending upon the nature of the material being accessed and the age of the pupils:

- Access to the Internet may be by teacher (or sometimes other-adult) demonstration.

- Pupils may access teacher-prepared information, rather than the open Internet.

- Pupils may be given a suitable web page or a single web site to access.

- Pupils may be provided with lists of relevant and suitable web sites, which they may access.

- Older, more experienced, pupils may be allowed to undertake their own internet search having agreed a search plan with their teacher; pupils will be expected to observe the Rules of Responsible Internet Use and will be reminded that checks can and will be made on files held on the system and the sites they access.

Pupils accessing the Internet are supervised by an adult at all times. They are only allowed to use the Internet once they have been taught the Rules of Responsible Internet Use and the reasons for these rules. Teachers endeavour to ensure that these rules remain uppermost in the children’s minds as they monitor the children using the Internet.

Using Information from the Internet

We believe that, in order to use information from the Internet effectively, it is important for pupils to develop an understanding of the nature of the Internet and the information available on it. In particular, they should know that unlike the school book collection for example, most of the information on the Internet is intended for an adult audience.

- Pupils will be taught to expect a wider range of content, both in level and in audience, than is found in a library or on TV.

- Teachers will ensure that pupils are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the Internet (as a non-moderated medium).

- When copying materials from the Web, pupils will be taught to observe copyright.

- Pupils will be made aware that the writer of an E-mail or the author of a web page may not be the person it is meant to be.

Maintaining the Security of the School ICT network

Being connected to the Internet significantly increases the risk that a computer or a computer network may be infected by a virus or accessed by unauthorised persons.
The ICT technician updates virus protection regularly, keeps up-to-date with IT news developments and works with the LA and Internet Service Provider to ensure system security. Strategies to protect the integrity of the network are reviewed regularly and improved as and when necessary.

Using E-mail & Blogs

Pupils learn how to use an E-mail/blog application and be taught E-mail/blog conversations. Staff and pupils use E-mail/blogs to communicate with others, to request information and to share information.

It is important that communications with persons and organisations are properly managed to ensure appropriate educational use and that the good name of the school is maintained. Therefore:

- Pupils may only use approved E-mail accounts on the school system.

- Pupils are only allowed to use E-mail/blogs once they have been taught the Rules of Responsible Internet Use and the reasons for these rules.

- Teachers endeavour to ensure that these rules remain uppermost in the children’s minds as they monitor children using E-mail/blogs.

- Children should not disclose their password to others

- Pupils may send E-mail as part of planned lessons.

- Incoming E-mail to pupils is not regarded as private.

- The forwarding of chain letters is not permitted. (The potential harm that can be caused will be included within Online Safety learning.)

- The use of social networking sites is not permitted and these sites will be blocked. Pupils and parents will be advised that the use of social networking spaces outside school is inappropriate for primary aged children. Staff and pupils should be advised not to publish specific and detailed private thoughts on social networking sites.

- Use of mobiles in school is not permitted. The sending of abusive or inappropriate text messages is forbidden.

- Pupils are not permitted to use E-mail/blogs at school to arrange to meet someone outside school hours.

Pupils' images or work

It is important that any content uploaded to the school website meets the following criteria:

- Images published to the web that include pupils will be carefully selected and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents and carers will be obtained before images of pupils are electronically published to the web.
- Pupil's work can only be published to the website with the permission of the pupil and the parents.

Cyber-bullying

Opportunities for pupils to bully or to be bullied via technology, such as E-mail, texts and messenger platforms and social media communities (i.e. Facebook, Whatsapp, Viber, FaceTime, Twitter, Snapchat and KIK) are becoming more frequent nationally. As such, teaching pupils about appropriate behaviours when using technology provides a vital grounding for future use. Whilst not wanting to provoke unrecognised opportunities in pupils, consideration must be given to suitable teaching and procedures to address any issues of cyber-bullying.

- The school's anti-bullying policy will address cyber-bullying. Cyber-bullying will also be addressed in ICT, PSHE and other relevant lessons and is brought to life through activities. As with other whole school policies, all staff and children will be included and empowered to take part in the process.

- Pupils, parents, staff and governors will all be made aware of the consequences of cyber-bullying. Young people and their parents will be made aware of pupils' rights and responsibilities in their use of new technologies and what the sanctions are for misuse.

- Parents will be provided with an opportunity to find out more about cyber-bullying through information sessions for parents.

- Holden Lane Primary will take all reasonable precautions to protect against cyber-bullying whilst pupils are in its care. However, due to the global and connected nature of new technologies, it is not possible to guarantee that inappropriate use via a school computer will not occur. Neither the school, nor Stoke on Trent City Council can accept liability for inappropriate use, or any consequences resulting outside of school.

Holden Lane Primary will proactively engage with pupils in preventing cyber-bullying by:

- Understanding and talking about cyber-bullying, e.g. Inappropriate use of E-mail, text messages etc.;
- Keeping existing policies and practices up to date with new technologies;
- Ensuring easy and comfortable procedures for reporting;
- Promoting the positive use of technology;
- Evaluating the impact of prevention activities.
- Records of any incidents of cyber-bullying kept and will be used to help to monitor the effectiveness of the school's prevention activities.

Managing Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out and protocols established before use in Holden Lane Primary is allowed.

Protecting Personal Data

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

Online Safety and Home/School Links

- A copy of the Online Safety policy is available for parents to read in the main reception area of school.

- Internet issues will be handled sensitively and parents will be advised accordingly.

- A partnership approach with parents will be encouraged. This could include parent sessions with demonstrations and suggestions for safe home Internet use.

- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

- The Online Safety Leader is willing to offer advice and suggest alternative sources of advice on the understanding that neither he/she, the school nor the LA can be held responsible for the consequences of such advice.

As noted above, it is not possible to be certain of the originator of an E-mail message, and for this reason the school is unable to accept an e-mail as parental authorisation of a pupil absence.

What to do if a problem arises

An adult uses IT equipment inappropriately.

- Ensure you have a colleague with you; do not view the misuse alone.
- Report the misuse immediately to the Headteacher and ensure that there is no further access to the PC or laptop.
- If the material is offensive, but not illegal, the Headteacher should then:
- Move the PC or laptop to a secure place.
- Instigate an audit of all ICT equipment by the schools ICT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.
- Take appropriate disciplinary action – contact HR.
- Inform governors of the incident.

In an extreme case where the material is of an illegal nature:

- Move the PC/laptop to a secure place and document what you have done.
- Contact the local police and follow their advice.

An inappropriate website is accessed unintentionally in the school by a teacher or child

A most important element of our Rules of Responsible Internet Use is that pupils are taught to tell a teacher **immediately** if they encounter any material that makes them feel uncomfortable.

If there is an incident in which a pupil is exposed to offensive or upsetting material, the school will respond appropriately to the situation quickly and if necessary, on a number of levels. Responsibility for handling incidents involving children will be taken by the Online Safety Leader and the Child Protection Officer, in consultation with the Headteacher and the pupil's class teacher. All the teaching staff will be made aware of the incident in Pupil Awareness at a staff meeting if appropriate.

- If one or more pupils discover (view) inappropriate material, our first priority will be to give them appropriate support. The incident will be reported to the Headteacher/Online Safety officer and the pupil's parents/carers will be informed if necessary, giving an explanation of the course of action the school has taken. The school aims to work with parents/carers and pupils to resolve any issue.

- If staff or pupils discover unsuitable sites the Online Safety Leader and school technician will be informed and the site will be filtered. The ICT Leader will report the URL (address) and content to the Internet Service Provider and the LA; if it is thought that the material is illegal, after consultation with the ISP and LA, the site will be referred to the Internet Watch Foundation and the police.

An inappropriate website is accessed intentionally by a child

Pupils are expected to play their part in reducing the risk of viewing inappropriate material by obeying the Rules of Responsible Internet Use, which have been designed to help protect them from exposure to Internet sites carrying offensive material. If pupils abuse the privileges of access to the Internet and E-mail facilities by failing to follow the rules they have been taught or failing to follow the agreed search plan when given the privilege of undertaking their own Internet search, then sanctions consistent with our School Behaviour Policy will be applied.

- The Online Safety Leader will be informed and reference will be made to the Acceptable Use Policy that was signed by the child and apply the agreed sanctions, this may include denied access to the Internet for a period of time.

- If necessary, inform parents/carers.

You find a pupil or adult logged on as someone else.

- Immediately log off the system.

- Determine whether the offending user had logged on with the permission of the owner of the username.

- Refer offender to the acceptable use policy that was signed by the user and apply agreed sanctions.

- Determine the extent to which anything inappropriate has been done.

- Contact Online Safety Leader and school technician to ensure passwords are changed immediately.

A bullying incident directed at a child occurring through email or mobile phone technology, either inside or outside of school time.

- Report to the Headteacher and Online Safety Leader.

- Advise the child not to respond to the message.

- Secure and preserve any evidence.

- Notify parents of the children involved.

- Inform the police (on request from LA/parents) if necessary and the Online Safety officer.

Malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

- Secure and preserve any evidence and endeavour to trace the origin

- Inform the Headteacher and Online Safety Leader who will then inform and request the comments be removed from the site.

- Headteacher and Online Safety Leader will collect all evidence and seek guidance from the LA Online Safety department.

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child.

- Report to Headteacher or other named child protection officer in the school who will contact parents, police and social services if necessary.

- Secure and preserve any evidence and advise the child on how to terminate the communication.