E-Safety

The Old School Henstead

Written by:	WJM/Reviewed by MJC
Last reviewed on:	24 Aug 2023
Next review due by:	24 Aug 24

E-safety Policy

1. Introduction

The school's e-safety policy relates to other policies including those for Anti Bullying, Child Protection and AUP. Our e-safety policy has been written and adapted by the school, building on best practice and government guidance. The e-safety policy and its implementation will be reviewed annually.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

Content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist, radical or extremist views;

Contact: being subjected to harmful online and offline interaction with other users; for example, commercial advertising as well as adults posing as children or young adults; and

Conduct: personal online and offline behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying.

This e-Safety Policy sets out the roles, responsibilities and procedures for the acceptable, safe, and responsible use of all digital and communication technologies, including the use of school-based devices, the internet, email, instant messaging and other social networking technologies and mobile phones and games, to safeguard adults and pupils. It details how the school will provide support and guidance to parents and the wider community (where appropriate) for the safe and responsible use of these technologies. It also explains procedures for any unacceptable use or misuse of these technologies by adults or pupils.

The use of the internet as a tool to develop teaching, learning and administration has become an integral part of school and home life. There are always going to be risks with using any form of communication which lies within the public domain. Therefore, it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst pupils use these technologies.

These risks include:

- Being vulnerable to inappropriate contact from strangers;
- Cyber-bullying;
- Illegal activities of downloading or copying any copyright materials and file-sharing via the internet or mobile devices;
- Issues with spam and other inappropriate email;
- Online content which is abusive, offensive, or pornographic;
- The use of social media to encourage extremism (see also: Prevent policy); and
- Viruses.

It is also important that staff are clear about the procedures, for example only contacting pupils about homework using school email addresses/ Google Classroom, not via personal emails.

Whilst we endeavour to safeguard and mitigate against all risks, we will never be able to completely eliminate them all. Any incidents that may come to our notice will be dealt with quickly and according to the school's policies to ensure the school continues to protect pupils.

It is the duty of the school to ensure that pupils, teachers, administrative staff and visitors are protected from potential harm whilst they are on school premises.

The involvement of pupils and parents is also vital to the successful use of digital technologies. This policy thus also aims to inform how parents and pupils are part of the procedures and how pupils are educated to be safe and responsible users so that they can make good judgments about information they see, find and use.

2. Aims of this Policy

- To ensure the safeguarding of all pupils within the school by detailing appropriate and acceptable use of all online and digital technologies.

 To outline the roles and responsibilities of all pupils, staff and parents.

 To ensure all pupils, staff and parents are clear about procedures for misuse of any online technologies.

 To develop links with parents and the wider community to ensure continued awareness of online technologies.

3. Pupils

3.1 Our pupils:

 Are taught to use the internet in a safe and responsible manner through, for example, ICT and PSHEE lessons;

 Are taught to immediately tell an adult about any inappropriate materials or contact from someone they do not know;

 Are made aware of the potential use of online digital technologies to expose young people to inappropriate contact from strangers and to extremist ideas and know what to do if they encounter such issues;

 Are taught and encouraged to consider the implications for misusing the internet and, for example, posting inappropriate materials to websites;

 Are taught that the downloading of materials, for example music files and photographs, needs to be appropriate and 'fit for purpose', based on research for school work, and be copyright free;

 Are taught to understand what is meant by e-safety through age appropriate delivery;

 Are taught that sending malicious or hurtful messages outside of the school can become a matter whereby the school may set sanctions or involve outside agencies such as the police;

 Are taught not to put themselves at risk online or through mobile phone use and taught what to do if they are concerned they have put themselves at risk;

 Are given explicit guidelines and procedures for using mobile phones and other personal devices in school and are expected to abide by this policy; and

4. Inappropriate Use by Pupils

Should a pupil be found to deliberately misuse digital or online facilities whilst at school, appropriate sanctions will be applied. If a pupil accidentally accesses inappropriate materials, the pupil is expected to report this to an appropriate member of staff immediately and take action to minimise the screen or close the window. Deliberate abuse or damage of school equipment will result in parents being billed for the replacement costs of the equipment. Should a pupil use the internet whilst not on the school premises in such a way as to cause hurt or harm to a member of the school community, the school will act quickly and in accordance with our Behaviour Policy

5 Staff

5.1 It is the responsibility of all adults within the school to:

- Adhere to the Staff Behaviour Policy including Computing Acceptable Use Policy;
- Be up to date with digital knowledge appropriate for different age groups;
- Be vigilant when using technology as part of lessons;
- Model safe and responsible use of technology;
- Provide reminders and guidance to pupils on Digital Safety;
- Ensure that pupils are protected and supported in their use of online technologies, and that they know how to use them in a safe and responsible manner;
- Not leave a computer or other device unattended whilst they are logged on;
- Lock away or safely secure all portable ICT equipment when not in use;
- Protect confidentiality and not disclose information from the network, or pass on security passwords;
- Make sure that any information subject to data protection legislation, , is not stored on unencrypted portable media or transported in an unsecure form;
- Use their discretion when communicating electronically about work-related issues and not bring the school's reputation into disrepute;
- Report any concerns about a pupil related to safeguarding and e-safety
- Report accidental access to inappropriate materials to the ICT Manager so that inappropriate sites are added to the restricted list;
- Only use school owned devices and memory cards to take photographs or videos.

6 Inappropriate Use by Staff

. If a member of staff is believed to have misused the internet or network in an abusive or illegal manner at school, a report must be made immediately to the Head and ICT Manager. Safeguarding procedures must be followed to deal with any serious misuse, a report filed, and all appropriate authorities contacted as necessary.

.

7 Parents and Visitors

. 7.1 All parents have access to a copy of this E-Safety Policy on our website. Parents are asked to explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted.

. 7.2 As part of the approach to developing e-safety awareness with pupils, the school may offer parents the opportunity to find out more about how they can support the school to keep their child safe whilst using online technologies beyond school; this may be by offering parent education sessions or by providing advice and links to useful websites.

The school wishes to promote a positive attitude to using the internet and therefore asks parents to support their child's learning and understanding of how to use online technologies safely and responsibly.

. 7.3 Parents should be aware that the school cannot take responsibility for a pupil's misuse or abuse of IT equipment when they are not on the school premises. This includes social networking with other pupils, and the possibility of pupils accessing inappropriate content. However, should parents or guardians become aware of an issue, we strongly encourage prompt communication with the school so we can offer advice and support. The school has a duty to report serious concerns to local authority safeguarding teams or to the police, in line with statutory requirements.

8 Video and Photography at School Events

Parents are asked to be considerate when taking videos or photographs at school events and are requested not to publish material of other children in any public forum without the permission of the relevant family.

. 8.1 Early Years Use of Mobile Phones or Device - Statutory Regulation

. 8.2 The Early Years Safeguarding and Welfare Requirements (para 3.4) requires all schools to have a clear policy on the use of mobile phones and devices.

. 8.3 The Staff Behaviour Policy/ Code of Conduct for Staff does not permit the use of personal mobile phones and cameras by staff where children are present.

9 The School's Responsibilities

9.1 The school takes its responsibilities in relation to the acceptable use of technology by pupils and adults seriously and understands the importance of monitoring, evaluating and reviewing its procedures regularly.

10 Filtering and Safeguarding Measures

. Anti-virus, anti-spyware, junk mail and SPAM filtering is used on the school's network, stand- alone PCs, laptops and tablets, and is updated on a regular basis. Security measures are in place to ensure information about our pupils cannot be accessed by unauthorised users. Strong encryption is used on the wireless network to provide good security.

11 Email Use

. All staff are expected to use email professionally and responsibly.

12 The School's Use of Images and Videos

. The school abides by data protection legislation, and understands that an image or video is considered personal data. It seeks written consent from parents to publish images or videos for external publicity purposes, such as the website, and for internal purposes. Parents and guardians may withdraw their permission at any time by informing the school in writing.

. .

13 The Curriculum and Tools for Learning

13.1 The school teaches our pupils how to use the internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding, and communicating effectively in order to further learning, through ICT and/or PSHEE lessons. The PSHE curriculum supports the teaching of E-Safety. The following concepts, skills and competencies are taught through the school in an age-appropriate manner:

- Digital citizenship;
- Future work skills;
- Internet literacy;
- Making good judgments about websites and emails received;
- Knowledge of risks such as viruses, and opening mail from a stranger;
- Access to resources that outline how to be safe and responsible.
- Knowledge of copyright and plagiarism issues;
- Awareness of age restrictions on common social media sites and games;
- Positive online communication which is not harmful or upsetting for others;
- Sharing personal information about themselves or others;
- File-sharing and downloading illegal content;
- Uploading information – knowing what is safe to upload.
- Where to go for advice and how to report abuse.

.

14 Monitoring

14.1 It is the responsibility of the school to ensure appropriate systems and technologies are in place to monitor and maintain the safeguarding and security of everyone using the school network. The school will monitor the use of online technologies and the use of the internet by pupils and staff.

15 Social Media

15.1 Access to social networking sites is not permitted in school. However, the school will advise pupils about their safe use e.g. use of passwords and appropriate age limits. Staff have received training on child-on-child abuse and 'youth produced sexual imagery' (commonly referred to as 'sexting') to develop their awareness of identifying concerning behaviours which may be linked to this issue. The training ensures that staff know how to respond to concerns in line with the school's Child Protection and Safeguarding policy.

16 Cyberbullying – Definition

16.1 Cyber bullying can be defined in the following terms:

Cyberbullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others.

Cyberbullying can involve Social Networking Sites, emails and mobile phones, used for SMS messages and as cameras.

The DfE advice Preventing and Tacking Bullying 2014 states that:

The rapid development of, and widespread access to, technology has provided a new medium for 'virtual' bullying, which can occur in or outside school. Cyber-bullying is a different form of bullying and can happen at all times of the day, with a potentially bigger audience, and more accessories as people forward on content at a click.

17 Cyberbullying – Preventative Measures

. 17. 1 We monitor pupils'use.

. 17.2 We may impose sanctions for the misuse, or attempted misuse of the internet.

. 17.3 We offer guidance on the safe use of social networking sites and cyberbullying

. 17.4 We offer guidance on keeping names, addresses, passwords, mobile phone numbers and other personal details safe.

. 17.5 Cyber-bullying will be covered in PSHEE lessons and during a focused Anti-Bullying week.

Mobile phones are not permitted in the School. In exceptional circumstances pupils, with the agreement of the Head, pupils may leave mobile phones with the Reception Office.

Wearable technology is not permitted in school.

COVID-19

In accordance with the latest government guidelines, the following hygiene precautions will be taken when using computing or digital equipment in school:

- All pupils will use hand sanitiser before and after using any computing or digital equipment.

- Headphones and computing equipment will be cleaned between year group use.

- Pupils will be reminded of expectations for online behaviour, bearing in mind that more time is likely to have been spent online and on social media during school closure. There may be an impact on friendship groups, emotional and mental well-being, which may stem from inappropriate use of IT. Any misuse of IT in this respect should be reported in the normal way as described above.

- The school recognises that following the long period at home where children have had more exposure online, closer monitoring will be required as well as a reminder of boundaries and expectations.