HERON CROSS PRIMARY SCHOOL

E-SAFETY POLICY

Date: February 2025

Review Date: January 2026

Contents

1. Statement of Intent
2. Legal Framework
3. Roles and Responsibilities
4. Curriculum
5. Technical – infrastructure / equipment, filtering and monitoring
6. Managing Reports of Online Safety Incidents

1. Statement of Intent

Heron Cross Primary School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement and enhancing teaching and learning.

The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff. The breadth of issues classified within online safety is considerable, but they can be categorised into three areas of risk:

- Content: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, and racist or radical and extremist views.

- Contact: Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults.

- Conduct: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

The policy statement applies to all staff, volunteers, children and young people and anyone involved in Heron Cross Primary School's operations.

2. Legal Framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

¤ The UK General Data Protection Regulation (UK GDPR)

¤ Data Protection Act 2018

¤ DfE (2021) 'Harmful online challenges and online hoaxes'

¤ DfE (2021) 'Keeping children safe in education 2020'

¤ Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'

¤ DfE (2019) 'Teaching online safety in school'

¤ DfE (2018) 'Searching, screening and confiscation'

¤ National Cyber Security Centre (2017) 'Cyber Security: Small Business

Guide'

▫ UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 editio

3. Roles and Responsibilities

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

Governors

Governors are responsible for the approval of the E-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. A member of the Governing Board has taken on the role of E-Safety Governor. The role of the Online Safety Governor will include:

- meetings with the E-Safety Co-ordinator
- regular monitoring of online safety incident logs
- reporting to relevant Governors

Headteacher and Senior Leaders

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the E-Safety Co-ordinator

The Headteacher and the 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. (See flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / other relevant body disciplinary procedures).

The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator / Officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator.

Online Safety/ E- Safety Coordinator:

The E-Safety Coordinator will take a day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents

The E-Safety Coordinator ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.

Acting as the named point of contact within the school on all online safeguarding issues.

Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.

Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.

Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.

Ensuring appropriate referrals are made to external agencies, as required.

Keeping up-to-date with current research, legislation and online trends and coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.

Maintaining records of reported online safety concerns as well as the actions taken in response to concerns. Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.

Working with the head teacher and governing body to update this policy on an annual basis.

ICT technicians

Provide technical support in the development and implementation of the school's online safety policies and procedures.

Implement appropriate security measures as directed by the Head teacher and Senior Leadership Team.

Ensure that the school's filtering and monitoring systems are updated as appropriate.

All staff members

Take responsibility for the security of ICT systems and electronic data they use or have access to.

Model good online behaviours.

Maintain a professional level of conduct in their personal use of technology.

Have an awareness of online safety issues.

Report concerns in line with the school's reporting procedure.

Where relevant to their role, ensure online safety is embedded in their teaching of the curriculum.

Pupils

Adhere to this policy and other relevant policies.

Seek help from school staff if they are concerned about something they or a peer have experienced online.

Reporting online safety incidents and concerns in line with the procedures within this policy.

4. Curriculum

Pupils

The education of pupils in online safety is 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.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited

Key online safety messages should be reinforced as part of a planned programme of assemblies

Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.

Staff should act as good role models in their use of digital technologies the internet and mobile devices

In lessons where internet use is pre-planned, it is best practice that 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.

Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need

Parents

Many 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 / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

Curriculum activities

Letters, newsletters, web site,

High profile events / campaigns e.g. Safer Internet Day

Reference to the relevant web sites/publications e.g.swgfl.org.uk, saferinternet.org.uk, www.childnet.com/parents-and-carers

Staff

All staff receive safeguarding and child protection training, which includes online safety training, during their induction. This online safety training for staff is updated annually and is delivered in line with advice from local safeguarding partners. In addition to this training, staff also receive regular online safety updates as required and at least annually.

All staff receive a copy of this policy upon their induction and are informed of any changes to the policy.

They understand the unique risks associated with online safety and be confident that they have the relevant knowledge and capability required to keep pupils safe while they are online at school.

They recognise the additional risks that pupils with SEND face online and offer them support to stay safe online. All staff are informed about how to report online safety concerns, in line with policy.

The Safeguarding Lead and any deputies undergo training to provide them with the knowledge and skills they need to carry out their role, this includes online safety training. This training is updated at least every two years. In addition to this formal training, the Safeguarding Lead and any deputies receive regular online safety updates to allow them to keep up with any developments relevant to their role. In relation to online safety, these updates allow the DSL and their deputies to:

5. Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.

There will be regular reviews and audits of the safety and security of school technical systems

Servers, wireless systems and cabling must be securely located and physical access restricted

All users will have clearly defined access rights to school technical systems and devices.

All users will be provided with a username and secure password by the technician who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password

The “master / administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe)

The technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations

Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes

Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.

The school has provided enhanced / differentiated user-level

School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement

An appropriate system is in place (children report to a member of staff and staff to report to headteacher/e-safety co-ordinator) for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).

Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

An agreed policy is in place (user restrictions – only ‘admin’ have the rights) that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.

Staff are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours.

Staff members are required to block spam and junk mail, and report the matter to ICT technicians. The school’s monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils are made aware of this. Chain letters, spam and all other emails from unknown sources are deleted without being opened.

Online safety learning organised where they explain what a phishing email and other malicious emails might look like – this assembly includes information on the following:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking “does the email urge you to act immediately?”
- The importance of checking the spelling and grammar of an email

Personal devices

Any personal electronic device that is brought into school is the responsibility

of the user.

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency and agreed with the SLT.

Staff members are not permitted to use their personal devices to take photos or videos of pupils.

Staff members report concerns about their colleagues' use of personal devices on the school premises.

If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the head teacher will inform the police and action will be taken.

Pupils are not permitted to use their personal devices during the school day.

Social networking -Personal use

Access to social networking sites is filtered as appropriate.

Staff and pupils are not permitted to use social media for personal use during lesson time.

Staff can use personal social media during break and lunchtimes in line with the mobile phone policy.

Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school.

Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media.

Where staff have an existing personal relationship with a parent or pupil, and thus are connected with them on social media, e.g. they are close family friends with a parent at the school, they will disclose this to the DSL and head teacher and will ensure that their social media conduct relating to that parent is appropriate for their position in the school.

Pupils are taught how to use social media safely and responsibly through the online safety curriculum.

Concerns regarding the online conduct of any member of the school community on social media are reported to the Safeguarding Lead.

The school's official social media channels are only used for official educational or engagement purposes.

All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

6. Managing Reports of Online Safety Incidents

Staff members and pupils are informed about what constitutes inappropriate online behaviour in the following ways:

- Staff training
- The online safety curriculum
- Assemblies

Concerns regarding a staff member's online behaviour are reported to the Head teacher who decides on the best course of action.

Concerns regarding a pupil's online behaviour are reported to the Safeguarding Lead who investigates concerns with relevant staff members.

Concerns regarding a pupil's online behaviour are dealt with in accordance with relevant policies depending on their nature.

Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The Safeguarding Lead will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response are recorded on CPOMS.