Online Safety Policy

Harvills Hawthorn Primary School

2024-2026

Reviewed January 2024

Introduction

This policy aims to outline the necessary procedures, behaviours and expectations which will improve the safety of children and staff in relation to the use of computers, mobile devices and any other technology.

We, as a school, recognise the growing concerns which are held by children, parents and educators about the risks and threats posed by technology which is, in many cases, readily available.

At Harvills Hawthorn Primary School, we have access to the internet through MacBooks, Windows computers, Chromebooks, iPads and Chrome Tablets. Therefore, this policy aims to ensure that these technologies and devices are used responsibly and safely to the end of ensuring safe use by staff and children alike. This policy applies to all children, all staff, all volunteers/ companies/ visitors/ students/ educators and anyone else who may use technology within school.

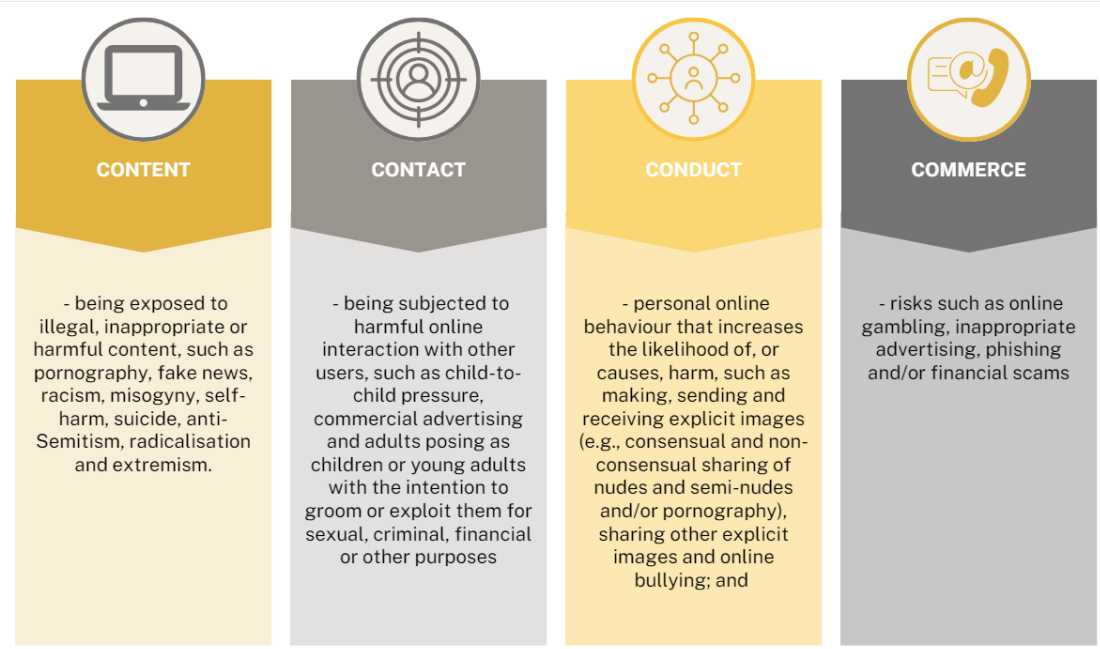
This policy has been written by the Online Safety coordinator (Daniel Westwood) and any safeguarding concerns, including those related to online safety, are dealt with by the head teacher and Designated Safeguarding Lead, Joanne Sheen.

We recognise the importance of safeguarding children from potentially harmful and inappropriate online material, and we understand that technology is a significant component in many safeguarding and wellbeing issues.

To address this, our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, and governors.
- Protect and educate the whole school community in its safe and responsible use of technology, including mobile and smart technology (which we refer to as ‘mobile phones’).
- Set clear guidelines for the use of mobile phones for the whole school community.
- Establish clear mechanisms to identify, intervene in and escalate any incidents or concerns, where appropriate.
- Adhere to the filtering and monitoring standards for schools and colleges (Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk) through the use of filtering and monitoring systems and processes, with regular analysis of their effectiveness in safeguarding the students whilst avoiding ‘over blocking’.

This policy aims to address the ‘4 C’s’ of online safety, as outlined in the Keeping Children Safe in Education document.



To meet our aims and address the risks above we will:

- Educate pupils about online safety as part of our curriculum. For example:
  - The safe use of social media, the internet and technology
  - Keeping personal information private
  - How to recognise unacceptable behaviour online
  - How to report any incidents of cyber-bullying, ensuring pupils are encouraged to do so, including where they are a witness rather than a victim.

- Train staff, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year.

- Educate parents/carers about online safety via our website, communications sent directly to them and during parents' evenings. We will also share clear procedures with them, so they know how to raise concerns about online safety.
- Make sure staff are aware of any restrictions placed on them with regards to the use of their mobile phone and cameras, for example that:
  - Staff are allowed to bring their personal phones to the school for their own use, but will limit such use to non-contact time when pupils are not present.
  - Staff will not take pictures or recordings of pupils on their personal phones or cameras.

- Make all pupils, parents/carers, staff, volunteers, and governors are aware that they are expected to sign an agreement regarding the acceptable

use of the internet in school, use of the school's ICT systems and use of their mobile and smart technology.

- Explain the sanctions we will use if a pupil is in breach of our policies on the acceptable use of the internet and mobile phones.

- Make sure all staff, pupils and parents/carers are aware that staff have the power to search pupils' phones, as set out in the DfE's guidance on searching, screening and confiscation

- Put in place robust filtering and monitoring systems to limit children's exposure to the 4 key categories of risk (described above) from the school's IT systems.

- Regularly review and assess the effectiveness of our filtering and monitoring systems to ensure they are fit for purpose and that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

- Ensure that alerts from our filtering and monitoring systems are received and reviewed by our DSL (or DDSLs in their absence) in order to be assured that safeguarding concerns are robustly responded (for example, alerts relating to risks of online radicalisation or online grooming)

- Carry out an annual review of our approach to online safety, supported by an annual risk assessment that considers and reflects the risks faced by our school community.

Use of digital technologies, devices and the internet within school.

The use of digital technologies, devices and the internet should adhere to the following guidelines. Generally, usage should seek to promote education, learning and engagement and not stray into illegal or harmful usage which causes risk. The school expects all users of the technologies, devices and the internet to understand and follow the policy in order to establish a safe and purposeful basis in which computing and technology can be explored.

Pupils who bring phones to school are not allowed to use them during the school day or on the school premises as they arrive/leave.

If a child brings a phone to school a parent/carer will need to complete a permission form and agree to the school's terms. Phones must be switched off and put in the designated box in the school office at the beginning and end of the day, pupils are not permitted to have devices on their person, in bags or lockers.

School is not liable for any loss or theft of mobile phones that pupils bring to school.

Pupils must adhere to the school's acceptable use agreement for mobile phone use

Users of the digital technologies, devices and internet within school should NOT:

- Visit internet sites, social media apps, make, post, download, upload or pass on material, comments or media which relates to:
    - Indecent images of children
    - Promoting discrimination of any kind
    - Promoting racial or religious hatred
    - Promoting illegal acts
    - Anything pornographic or sexual in nature
    - Anything which may cause offense to peers, staff or students

Sometimes, some of these areas may arise when exploring or browsing sites. When/if this happens, advise children (if they are involved) on how to deal with happening upon inappropriate material and later report the incident to the online safety coordinator, Mark Edwards, computer technician, or the designated safeguarding lead.

However, if there are incidents whereby deliberate access to websites, online forums or groups or articles which pertain to any of the following areas has been carried out, then the incident should be reported to the police:

- Images of child abuse
- Adult material which breaches the Obscene Publications Act
- Criminally racist or anti-religious material
- Violence and bomb making
- Illegal taking or promotion of drugs
- Software piracy
- Material related to terrorist activity or propaganda

In addition to this, users may also not use the school's broadband services in the following manners or instances:

- To run a private business
- Enter into personal transactions that involve the school
- Visit sites which may be defamatory or incur liability or adversely impact upon the image or reputation of the school or associated partners
- Use, upload, download or transmit copyrighted material
- Reveal confidential information, which includes but is not limited to: financial information, personal information, databases, computing access codes, business relationships.
- Intentionally interfere with the normal operation of the Internet connection
- Use the internet to reveal personal opinions which could be considered inappropriate or offensive
- Violate the privacy of others
- Corrupting or deleting others' data within prior permission

- Continue to use a device or item after request to desist because it is causing technical, safety, privacy or other issues
- Use technologies to intimidate, threaten or cause harm to others
- Use technology, either owned by the school or yourself, to take images or videos of children which are then taken out of the school premises (i.e. images or videos of children should not be stored on a device which will leave the school grounds).

Reporting abuse

Cyberbullying and sexting by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures.

Serious incidents may be managed in line with our Safeguarding and Child Protection procedures.

- Any abuse suffered by children or staff should be reported to the SLT.
- Where possible, evidence (screenshots, recordings etc.) should be kept and used to report the incident
- If the abuse is of a criminal nature, then it should, along with any relevant evidence, be reported to the police service.

Education and Training

We recognise the importance of a sound, thorough and purposeful education about the key elements of online safety relevant to the lives of the young people we teach. It is crucial that we ensure all children have an understanding of the risks posed by the use of online technologies, the consequences of their actions and decisions and the steps they can take to seek help, guidance and safety if instances occur which make them uncomfortable, anxious or fear for their or others' safety.

To this end, we ensure that online safety learning forms a crucial and paramount aspect of our computing curriculum. We have created a specific online safety curriculum which is based upon the document 'Education for a Connected World'. Each year group has a structured set of targets which will be taught throughout the academic year. These targets also specifically address each of the '4 C's' of online safety, as outlined in the Keeping Children Safe in Education document.

This curriculum will aim to teach children about various aspects of online safety, including teaching about how to use social media responsibly and to an age-appropriate level, about the dangers of cyberbullying and how to counteract it and about how 'sexting' can be damaging and dangerous (to an obviously age-appropriate level).

In order to deliver these targets effectively, teachers will be expected to deliver a class assembly, on a weekly basis, in relation to the targets outlined in their curriculum. Additionally, it is an expectation that key online safety messages are revisited each time teachers use technological equipment with

their class. Furthermore, online safety is a key theme within our annual Safety Week and we also engage with Safer Internet Day as a school too. Therefore, children are exposed to a wealth of opportunity to learn, discuss and engage with online safety learning. Finally, through our RSHE and PSHE curriculum, we also deliver a Computer Safety topic via One Decision for each year group every year, which also covers key aspects of the Online Safety Curriculum too.

In order for staff to deliver this wealth of online safety coverage adequately, they are frequently trained on new or topical online safety points. Every year, staff undertake safeguarding training and online safety forms part of this training. Also, at least once a year, staff receive explicit online safety training. Staff are made aware of practices, procedures, relevant information and where to find additional resources or information to further their knowledge.

As a school, we also understand the importance of educating and engaging with parents. We aim to provide updates on online safety issues through our distribution of newsletters or explicit communications, which inform parents of relevant issues. This is usually undertaken via e-mail or text message, whereby relevant threats, issues or knowledge are shared using produced materials, online links or information sheets. Much of this content comes from the platform, National Online Safety, which we subscribe to as a school in order to enable updated information and advice to accessed and distributed with ease and clarity.

Filtering and Monitoring

The use of technology within school (by children) is always supervised by adults. As well as this ‘over the shoulder’ approach, all of our devices are equipped with forensic software, Impero, which is always scanning for key words which are identifiers for inappropriate or worrying use. If one of these key words is typed or searched for, a screenshot is taken and sent to the DSL, Joanne Sheen and two named DDSLS, along with the time of the incident. The breach will then be investigated and, if necessary, the incident will be dealt with following our safeguarding procedures.

We take very seriously our responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, and implementing filtering and monitoring systems and processes is a key part of this.

We adhere to the government standards published in: Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

Filtering and Monitoring systems enable us to limit as much as possible, children’s exposure to the online risks from the school’s IT system.

At this school, we use the following system/s: Sandwell LA Firewall to filter and Impero to monitor.

Online Safety and Filtering and Monitoring is the responsibility of the DSL. They are supported in this by the governing body and together, they review the effectiveness of the systems, at least on an annual basis. We use a range of tools to help us review, including the Prevent Duty risk assessment.

It is vital that Filtering and Monitoring helps us to keep children safe but does not lead to 'over blocking' – creating unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

Examples could be children being unable to access factual information relating to a project or being blocked from accessing helpful resources and websites to seek support.

Staff working with children are in key positions to notice if there are any concerns and to escalate these immediately to the DSL, recognising them as a potential safeguarding concern. Examples of this include (but are not limited to):

- Spotting or overhearing that students have managed to override a system and access inappropriate content online.
- Spotting or overhearing students being able to use slang terms that are not recognised by the filtering and monitoring system and using these to search for and access inappropriate content.
- Spotting that inappropriate settings have been placed on video-sharing sites such as YouTube enabling for harmful or inappropriate videos to be accidentally shared with students.

Our filtering and monitoring system sends us daily alerts of when a child may have attempted to access harmful or inappropriate content.

These are monitored and responded to as they arise by:
Miss Sheen, Miss Soper and Mr Griffiths.

Additionally, Miss Sheen is responsible during school holidays or outside of school hours.

In their absence, the member/s of staff who will take on this responsibility are:
Senior Leaders present in school.

Upon receiving a filtering and monitoring alert or notification, the DSL or a deputy will consider whether there is any risk to the child or whether further support may be necessary, taking into account any contextual or historical concerns on the child's safeguarding file, or any current risk assessments. Action may be taken, as with any safeguarding concern, including (but not limited to):

- Liaison with other professionals working with the child such as Police, Children's Social Care, CAMHS/CYPMHS
- Liaison with parents/carers

- Actioning another member of staff such as class teacher, a member of the pastoral team or mentor to speak further with the child and explore support options.

Sanctions

If a child is seen to be misusing technology or using technology in a way which is deemed worrying, concerning, harmful or abusive, then appropriate steps will be taken in line with the school's behaviour and safeguarding policies.

If the incident is serious enough in nature, the children's parents will be informed and/or their use of technology may be suspended or withdrawn for their and others' safety and wellbeing.

If staff are known, seen or proven to be misusing technology, then this shall be reported to the head teacher in line with the low-level concerns policy. If the staff are found to be in breach of any school policies, including this one, then disciplinary procedures may be undertaken. If the incident is serious in nature, then incidents may be passed to the police or child protection services.

It is important that all staff are responsible for their own actions but also for monitoring and reporting worrying actions witnessed by other members of staff to ensure the safety of all children and staff within school.

Organisations for Support regarding Online Safety

www.thinkuknow.co.uk: CEOP's Online Safety resource and education advice

disrespectnobody: Home Office advice on Healthy Relationships including sexting and pornography

UK Safer Internet Centre: Contains a specialist helpline for UK schools and colleges

Internet Matters: Advice for Parents on how to keep their children safe online

Parentzone: Advice for Parents on how to keep their children safe online

Childnet Cyberbullying: Guidance for schools on Cyberbullying

PSHE association: Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images

Educate Against Hate - Prevent Radicalisation & Extremism: Practical Advice

for Parents/Teachers and Governors on protecting children from extremism and radicalization

The use of social media for online radicalisation - GOV.UK (www.gov.uk): A government briefing for schools on how social media is used to radicalise young people

Overview_of_Sexting_Guidance.pdf (publishing.service.gov.uk): UK Council for Internet Safety (UKCIS) guidance on dealing with sexting incidents.

E-safety for schools | NSPCC Learning: NSPCC resources for schools on teaching Online Safety

Common Sense Media: Age-Based Media Reviews for Families | Common Sense Media: Common Sense Media gives advice for parents and carers on choosing age-appropriate online games and sites for their child.

Searching, screening and confiscation at school - GOV.UK (www.gov.uk): A government briefing on searching and confiscation of devices within schools

The National Grid for Learning - Safeguarding (google.com): Advice for schools from the London Grid for Learning

This policy should be read alongside our Safeguarding and Child Protection Policy.