



# Hardwick and Cambourne Community Primary School

## Online Safety Policy

Date Reviewed: Summer 2025  
Reviewed by: Governing Body  
Next Planned Review: Summer 2027



## **Safeguarding Statement**

At Hardwick and Cambourne Community Primary School we respect and value all children and are committed to providing a caring, friendly and safe environment for all our pupils so they can learn, in a relaxed and secure atmosphere. We believe every pupil should be able to participate in all school activities in an enjoyable and safe environment and be protected from harm. This is the responsibility of every adult employed by, or invited to deliver services at Hardwick and Cambourne Community Primary School. We recognise our responsibility to safeguard all who access school and promote the welfare of all our pupils by protecting them from physical, sexual and emotional abuse, neglect and bullying.

## Statement of intent

Hardwick and Cambourne 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 four areas of risk:

- Content: Being exposed to illegal, inappropriate or harmful material, e.g. fake news, self-harm and suicide, and discriminatory or extremist views.
- Contact: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- Conduct: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- Commerce: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

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.

## Legal framework

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

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2022) 'Keeping children safe in education 2022'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- 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'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'

## Roles and responsibilities

The governing board is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The named subject leader is responsible for:

- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Ensuring the curriculum coverage is sufficient for online safety.
- Reviewing the curriculum on a regular basis
- Ensuring staff have a good understanding of how to teach online safety including having a knowledge of particular technologies children may use at home.

### Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the headteacher and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

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

### Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with in line with the Anti-bullying Policy.

### Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age. The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Up skirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour.

## **Mental health**

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation. The school computing curriculum and the emotions for learning curriculum support children in learning ways of looking after their mental health in relation to technology.

## **Online safety training for staff**

The DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life. Information about the school's full responses to online safeguarding incidents can be found in the Anti-bullying Policy and the Child Protection and Safeguarding Policy.

## **Online safety and the curriculum**

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- Computing
- PSHE
- RSE

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem
- Consent, e.g. with relation to the sharing of indecent imagery or online coercion to perform sexual acts
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age inappropriate

The online risks pupils may face online are always considered when developing the curriculum.

## **Use of technology in the classroom**

A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- iPads
- Email
- Cameras

The computing lead has reviewed all technology in school ensure that it is safe for pupil and staff use. The school uses a tracking system which notifies the DSL if there are any online safety breaches for pupils or adults in the building.

## **Internet access**

Staff and other members of the school community are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A record is kept of users who have been granted internet access in the school office.

### **Filtering and monitoring online activity**

Hardwick and Cambourne primary School uses Netsweeper as its filtering and monitoring systems. The filtering and monitoring systems the school implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.

Deliberate breaches of the filtering system are reported to the DSL and DDSL, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be dealt with in line with the school's Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices are appropriately monitored. All users of the network and school-owned devices are informed about how and why they are monitored. Concerns identified through monitoring are reported to the DSL who manages the situation in line with the Child Protection and Safeguarding Policy.

### **Network security**

Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT technicians. Firewalls are switched on at all times. ICT technicians review the firewalls on a monthly basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments, and are expected to report all malware and virus attacks to ICT technicians.

All members of staff have their own unique usernames and private passwords to access the school's systems.