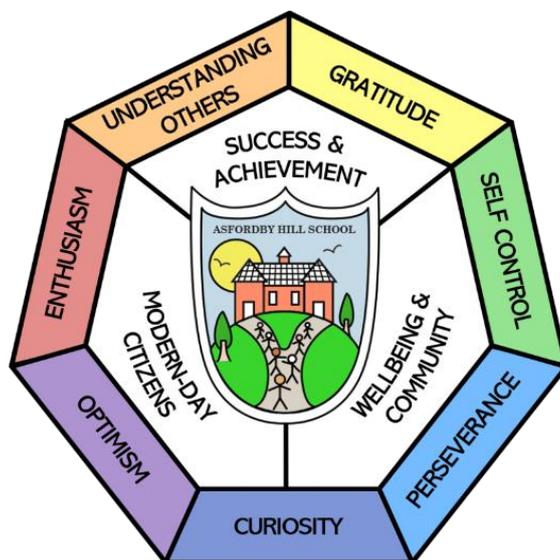


# Asfordby Hill Primary School

## *Online Safety, Filtering and Monitoring Policy*



### *Individual Value; Valuing Individuals*

#### **Our Vision & Aims:**

<b><u>Success &amp; Achievement</u></b>	<b><u>Modern-Day Citizens</u></b>	<b><u>Wellbeing &amp; Community</u></b>
<ol style="list-style-type: none"> <li>1. All children have their personal success celebrated.</li> <li>2. All children achieve highly, regardless of background.</li> <li>3. All children are resilient, respectful and confident learners.</li> </ol>	<ol style="list-style-type: none"> <li>4. All children leave with deep, flexible knowledge.</li> <li>5. All children leave literate, including digital literacy.</li> <li>6. All children experience a rich, broad and balanced curriculum built on foundational British values.</li> </ol>	<ol style="list-style-type: none"> <li>7. All children are happy and safe at school.</li> <li>8. All children equipped to take charge of their own wellbeing.</li> <li>9. All children experience an excellent personal development program.</li> </ol>

#### **Policy Links:**

KCSIE, PREVENT, Staff Code of Conduct, Computing Policy, Teaching and Learning Policy, PSHE

#### **Recommended or Statutory**

**Date Reviewed:** Sep 2025

**Date of Next Review:** Sep 2026

**Committee Responsible for Review:**

QEHS

**Signature of the Chair of Governors:**

4/11/25

# 1. Purpose

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices;
- provide staff and volunteers with the overarching principles that guide our approach to online safety; and
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

The policy statement applies to all staff, volunteers, children and young people and anyone involved in Asfordby Hill Primary School's activities.

## 2. Introduction

The use of technology has also become a significant component of many safeguarding issues, including cyberbullying, child sexual exploitation, radicalization and sexual predation. Unfortunately, technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.

### 2a. The Prevent Duty

Schools and registered childcare providers in England and Wales are required to, under 'The Prevent Duty', to ensure children are safe from terrorist and extremist material when accessing the internet in schools and should ensure that suitable filtering is in place.

### 2b. Keeping Children Safe in Education

The Department for Education's statutory guidance 'Keeping Children Safe in Education (KCSIE)' obliges schools in England to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or college's IT system" however, schools will need to be careful that over blocking does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

Furthermore, under KCSIE, as part of safeguarding and child protection training, all staff should understand their responsibility in relation to online safety which includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring, including as part of their induction. Additionally, online safety updates (as part of other child protection and safeguarding updates) are required to be provided to staff at least annually.

Updated KCSIE guidance (2025) now places emphasis that the designated safeguarding lead (DSL) must take lead responsibility for online safety as part of their safeguarding and child protection responsibility - this includes understanding the filtering and monitoring systems and processes in place.

### 2c. OfSTED

Whilst internet filtering has always been provided by schools, it is the 'strengthened measures' that are now a key part of Ofsted online safety during inspections.

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part by the risk assessment required by the Prevent Duty.

### 3. Online Safety, Filtering and Monitoring

#### 3a. Online Safety Risks

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorized into four areas of risk:

1. **Content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism
2. **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
3. **Conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying
4. **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (<https://apwg.org/>)

#### 3b. Filtering and Monitoring

##### Department for Education (DfE)

The DfE makes it clear the standards that schools should meet as regards filtering and monitoring in schools:

- roles and responsibilities to manage filtering and monitoring systems should be identified and assigned;
- filtering and monitoring provision should be reviewed at least annually;
- the filtering system should block harmful and inappropriate content without unreasonably impacting teaching and learning; and
- monitoring strategies should be effective and meet the safeguarding needs of the school.

Further guidance can be found here on how to meet the standards:

<https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges>

#### Schools Broadband and Netsweeper

Schools Broadband is our internet service provider and they provide the school with Netsweeper, an advanced content filtering platform that allows schools to monitor, block and report harmful content online. Devices that do not require logging into, such as iPads, experience the highest level of restrictions placed onto the internet by Netsweeper. Other filters of varying levels of restriction are deployed when users log into a device (PC or Laptop, for example) through the user management system – Microsoft Azure – through “groups”, managed by our IT management company, which means that students experience higher levels of restriction, whereas staff experience a slightly lesser level of restriction. Varying levels of filtering can also be applied to specific devices through IP address filtering.

All blocking of websites through the filters are at the discretion of the headteacher and written approval must be obtained before the IT management company are able to unblock any websites.

All internet usage is monitored by Schools Broadband and Netsweeper, and regular reports are provided to the IT management company, designated safeguarding lead and the ICT/computing lead who are able to take action accordingly.

### **Monitoring Systems**

Daily, all classroom staff and volunteers working with children will monitor children's usage of internet within lessons, remaining vigilant to ensure the safety of the children. Staff will report any breaches of filtering or concerns through the agreed reporting systems.

Annually, leaders will monitor filtering by completing a check that filters are working effectively using South West Grid for Learning resources (<http://testfiltering.com/>) and conduct a wider filtering and monitoring check (including logging into various stakeholder accounts to check that filters work appropriately at all levels) and ensure that record is kept ([FILTERING AND MONITORING CHECKLIST MASTER.docx](#)).

## **4. Roles and Responsibilities**

Appendix A provides detail of who assumes each of the roles below.

### **4a. The Governing Body**

- i. The Governing Body should ensure that online safety is a running and interrelated theme whilst devising and implementing their whole school approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected in relevant policies, the curriculum, teacher training, the role of the designated safeguarding lead (and deputies) and any parental engagement.
- ii. The elected safeguarding governor assumes responsibility for online safety, filtering and monitoring as part of their wider safeguarding role.

### **4b. Headteachers**

- i. The headteachers and appropriate members of the senior leadership team, are responsible for ensuring that this policy is adhered to, and that:
  - Their school has appropriate filters and monitoring systems in place, whilst considering their responsibility to safeguard and promote the welfare of children, and provide them with a safe environment in which to learn.
  - They consider the age range of their pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks.
  - Leaders conduct a risk assessment as required by the Prevent Duty.
  - The school keeps updated of statutory changes of government policy, and that the school meets all legal requirements for online monitoring and filtering.
  - The school implements the relevant statutory arrangements for online monitoring and filtering.
- ii. The headteachers are responsible for approving requests to the IT management company to unblock sites and is responsible for ensuring that a record is kept of changes to filtering systems by the IT management company.

### **4c. Designated Safeguarding Lead / Deputy Designated Safeguarding Lead**

- i. The designated safeguarding lead and deputy will assume lead responsibility of online safety as part of their wider child protection and safeguarding responsibilities, including taking action when online safety related safeguarding concerns are reported.
- ii. They will provide online safety updates (as part of other child protection and safeguarding updates) to staff at least annually.

- iii. They will include online safety in their wider safeguarding reporting to governors.
- iv. They will lead an annual check of filtering and monitoring and keep a record.

#### 4d. IT Management Company and IT Service Provider

- i. The IT Service Provider assumes technical responsibility for:
  - maintaining filtering and monitoring systems;
  - providing filtering and monitoring reports; and
  - completing actions following concerns or checks to systems.
- ii. The IT Management Company maintains responsibility for sending filtering and monitoring reports to the DSL, and IT and computing leader. They maintain responsibility for receiving written approval from the headteacher before unblocking websites as part of the filtering systems when requested to by other staff members and keeping a written record of all changes to filtering systems.

#### 4e. IT and Computing Lead

- i. The IT and computing lead will ensure that all teaching and support staff are knowledgeable in relation to online safety and receive appropriate training where needed to deliver and teach online safety effectively.
- ii. They will ensure that teaching staff are aware of and have implemented systems in relation to online safety in the classroom:
  - a. A system for monitoring users of iPads must be in place, including keeping records of who has used iPads and when.
  - b. The creation of an agreement to an “online safety charter” (see Appendix B). This should be on display in classrooms.
- iii. They will ensure that online safety is taught as part of the wider computing curriculum at school and regularly review the effectiveness of this.

#### 4f. All other staff

- i. Teaching staff are responsible for the implementation of systems in regards to online safety within their classrooms:
  - a. A system for monitoring users of iPads must be in place, including keeping records of who has used iPads and when.
  - b. All classes, within their first computing lesson of the year (and reviewed as appropriate), should create and agree to an “online safety charter” (see Appendix B). This should be on display in classrooms.
- ii. All other staff will be vigilant in their duty to safeguard children in terms of monitoring children’s usage of the internet in school.
- iii. They will ensure that they follow the school’s code of conduct with regard to appropriate use of the internet and that they alert leaders to any breaches in filtering and monitoring systems promptly.
- iv. They will report any safeguarding concerns through the school’s agreed procedures – this includes children accessing content through the internet that poses a risk to them (see section 3, online safety risks, for a non-exhaustive list).

#### 4g. Visitors and Members of the Community

Visitors and members of the community who use the school’s ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms.

## 4h. Parents / Guardians

Parents / guardians are expected to:

- Notify a member of staff or the headteachers of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

<https://www.childnet.com/help-and-advice/parents-and-carers>

<https://saferinternet.org.uk/guide-and-resource/what-are-the-issues>

## 5. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

The information below is taken from the National Curriculum computing programmes of study. It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All primary schools have to teach: • Relationships education and health education in primary schools.

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content

By the end of primary school, pupils will know:

- That the internet can be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- That people sometimes behave differently online, including by pretending to be someone they are not

- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing

- Why social media, computer games and online gaming have age restrictions and how to manage common difficulties encountered online
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private

How AI has many uses to help learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

- Where and how to report concerns and get support with issues online

The safe use of social media and the internet will also be covered in other subjects (such as PSHE e.g. through KidSafe) where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Reviewed:

- 2nd September 2024 (updated to reflect KCSiE 2024)
- 2nd September 2025 (updated to reflect KCSiE 2025, local and national guidance)

Appendix A: Table of Assumed Roles

<b>Role</b>	<b>Who?</b>
Governing Body	All members of the governing body
Designated Safeguarding Governor	Tanya Davis
Headteachers	Phil Millward /Nicola Bailey
Designated Safeguarding Lead	Phil Millward
Deputy Designated Safeguarding Lead	Nicola Bailey/Louise Parrott
IT Service Provider	Schools Broadband
IT Management Company	ICTTechie – James Crowhurst
IT and Computing Lead	Declan Forde
All Other Staff	All other teaching, support and non-teaching staff - including office and premises staff.

Appendix B: Sample Online Safety Charter



In our class, we try our best to be safe and secure while using technology, particularly the internet.

**1** We only use apps and websites that our teacher has directed us to use.

**2** If our teacher has asked us to research something, we only search using words related to our learning.

**3** I will respect other people digital artefacts. I will not delete, edit or do anything to others' work that may upset them.

**4** I will not share any personal information (name, age, school name, etc.) on the internet - including on Scratch.

I will be honest, responsible and accountable.

If I break this agreement, or see others breaking the agreement, I will be honest with my teacher.