Vernham Dean Gillum's C of E Primary School

Online Safety Policy

(Statutory Safeguarding, Filtering & Monitoring, AI Safety & Child Protection Policy)

Date of Policy: September 2026	**Date for Review: September 2027**
Status: Statutory Safeguarding Policy	**Framework: Keeping Children Safe in Education (KCSiE 2026), Meeting Digital and Technology Standards in Schools, the Data (Use and Access) Act 2025, the Data Protection Act 2018, and the UK GDPR.**

1. Aims of the Policy

The purpose of this policy 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, artificial intelligence (AI), or mobile devices.
- Provide staff, governors, and volunteers with the overarching principles that guide our approach to online safety, filtering, monitoring, and digital literacy.
- Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices, data, and emerging technologies.

This policy statement applies to all staff, governors, volunteers, children, and young people, and anyone involved in Vernham Dean Gillum's C of E Primary School's activities.

2. Legal Framework & Safeguarding Principles

This policy has been drawn up on the basis of legislation, statutory guidance, and national standards seeking to protect children in England, including Keeping Children Safe in Education (KCSiE 2026), Meeting Digital and Technology Standards in Schools, the Data (Use and Access) Act 2025, the Data Protection Act 2018, and the UK GDPR. Summaries of key guidance are accessible via NSPCC Learning.

We believe that:

- Children and young people should never experience abuse of any kind.
- Children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- The online world provides everyone with many opportunities; however, it can also present risks and challenges (including cyberbullying, grooming, radicalisation, online misogyny/misandry, sexual harassment, and AI-enabled abuse).
- We have a duty to ensure that all children, young people, and adults involved in our school are protected from potential harm online.
- We have a statutory responsibility to help keep children safe online, whether or not they are using Vernham Dean Gillum's C of E Primary School's network and devices.
- Working in partnership with children, young people, their parents, carers, and external agencies is essential in promoting pupil welfare and supporting responsible digital citizenship.
- All children, regardless of age, disability, gender reassignment, race, religion or belief, sex, or sexual orientation, have the right to equal protection from all types of harm or abuse.

Contextual Safeguarding Considerations:

To ensure equal protection, staff receive tailored guidance and resources addressing specific pupil groups, including:

- Safeguarding children from Black, Asian, and minoritised ethnic communities.
- Safeguarding d/Deaf and disabled children and young people.
- Safeguarding LGBTQ+ children and young people.
- Safeguarding children with Special Educational Needs and Disabilities (SEND).

3. Operational Online Safety Commitments

Vernham Dean Gillum's C of E Primary School seeks to keep children and young people safe by:

- Appointing an **Online Safety Coordinator** / **Designated Safeguarding Lead (DSL)** who oversees the school's online safety strategy, supported by PSHE schemes of learning and NSPCC guidance.
- Providing clear and specific directions to staff and volunteers through our Staff Code of Conduct and Acceptable Use Policy (AUP).
- Supporting and encouraging young people to use the internet, social media, and digital tools safely, critically, and respectfully.
- Supporting parents and carers with resources and guidance to promote online safety in the home.
- Maintaining clear, robust procedures to respond effectively to any incidents of inappropriate online behaviour or digital harm.
- Regularly reviewing and updating the security of our information systems, ensuring logins, email accounts, and passwords are managed securely.
- Ensuring personal data is processed securely in compliance with the Data (Use and Access) Act 2025 and UK GDPR.
- Operating a strict Zero-Online Pupil Image Policy across public digital platforms, ensuring no identifiable student faces are published online, and obtaining written consent for all internal media uses.
- Risk assessing new technologies, software, social platforms, and Generative AI systems prior to educational deployment.

4. Generative Artificial Intelligence (AI) and Emerging Technologies

- **Acceptable Use of AI:** Staff and pupils using AI systems for educational purposes must ensure compliance with data privacy regulations. No personal, sensitive, or identifiable pupil data or work may be inputted into public AI models.
- **AI-Enabled Harm & Deepfakes:** The creation, manipulation, or distribution of synthetic nudes, semi-nude images, deepfakes, or sexually explicit material using Generative AI is strictly prohibited. Any incident involving AI-generated image abuse or sexual harassment will be managed immediately as a severe safeguarding incident requiring a formal risk assessment under Child-on-Child Abuse protocols.

5. Filtering and Monitoring Standards

Vernham Dean Gillum's C of E Primary School uses robust filtering systems to block access to illegal and inappropriate content, including pornography, violence, hate speech, extreme views, radicalisation, and self-harm materials. Our internet filtering is delivered via Watchguard in partnership with our IT service provider, Harrap IT.

We actively monitor pupil online activity across school systems using a combination of methods:

- **Network Monitoring:** Network Traffic Monitoring: Automated analysis of network traffic to flag suspicious or harmful connections.
- **Device Monitoring:** Device-Level Monitoring: Monitoring software installed on devices connected to the school infrastructure.
- **Physical Supervision:** Active Physical Supervision: Direct staff supervision of pupil screens during digital learning activities.

Governance and Annual Review:

In accordance with KCSiE requirements, a named member of the Senior Leadership Team (SLT), alongside the DSL and Harrap IT, conducts a mandatory **Annual Filtering and Monitoring Review**. Written records of system tests, risk assessments, and blocklist audits are maintained and reported annually to the Governing Body.

6. Responding to Online Abuse & Cyberbullying

If online abuse or a digital safeguarding incident occurs, the school will respond by:

- Executing established child protection and safeguarding procedures immediately.
- Logging all concerns promptly on CPOMS. Incidents involving sexting, youth-produced sexual imagery, or AI deepfakes will follow statutory triage guidance without viewing, copying, or forwarding imagery unnecessarily.
- Providing comprehensive support and training for staff and volunteers on managing all forms of online abuse, cyberbullying, sexual harassment, and digital exploitation.

- Ensuring responses prioritize the wellbeing, dignity, and safety of the victim, bystanders, and the wider school community.
- Reviewing intervention plans at regular intervals to ensure long-term resolution and victim support.

> **Emergency Incident Triage & Key Reporting Pathways**
>
> In the event of severe online abuse, AI image manipulation, or sexual extortion, activate the following statutory pathways immediately:
>
> - **Local Police / 999:** Contact Hampshire Constabulary immediately if a child is at immediate risk or if illegal AI CSAM is generated/distributed.
> - **Hampshire LADO:** Report statutory allegations or adult concerns to the Local Authority Designated Officer (01962 876364).
> - **Under 18s Takedowns:** Assist pupils with 'Report Remove' (Childline/IWF) or 'Take It Down' (NCMEC) to remove intimate images.
> - **Staff & Professional Support:** Access the Professionals Online Safety Helpline or Stop It Now! for advisory support.

7. Additional Filtering and Monitoring Guidance for Parents

Parents and carers can implement home filtering and monitoring controls to reinforce digital safety outside of school. When choosing home software, families should consider:

- **Age Appropriateness:** Selecting tools appropriate for the child's developmental stage.
- **Device Compatibility:** Ensuring filtering software covers mobile phones, tablets, gaming consoles, and smart TVs.
- **Budget Options:** Exploring free built-in parental controls offered by internet service providers (ISPs) and device operating systems.

Practical Tips for Parents:

- Engage in open, regular conversations with children about their online activities and digital relationships.
- Establish family rules for screen time, device-free zones, and acceptable app usage.
- Utilize built-in parental controls to filter explicit content and manage screen time limits.
- Encourage critical thinking regarding online content, social media trends, and AI-generated media.
- Reassure children that they can speak to a trusted adult if they encounter upsetting content online.

8. Related Policies and Procedures

This policy statement should be read in conjunction with the following school policies and procedures:

- Child Protection and Safeguarding Policy

- Procedures for responding to concerns about a child or young person's wellbeing
- Dealing with allegations of abuse made against a child or young person
- Managing allegations against staff and volunteers
- Code of conduct for staff and volunteers
- Behaviour & Anti-Bullying Policy
- Child-on-Child Abuse Policy
- Photography and image sharing guidance
- Data Protection & GDPR Policy