PRINCE'S MEAD

E-SAFETY POLICY

Author:	Mrs Saffi Mant (Head of Digital Learning)
Date:	February 2026
Review Frequency:	Annual
Next Review Date:	February 2027
Sub-Committee:	Education

Compliance Checklist

- Policy reviewed annually and approved by Governing Body
- Staff trained on online safety and filtering responsibilities
- DSL and IT support review filtering and monitoring reports termly
- Random 'Dip Tests' completed on devices
- IT systems checked for filtering effectiveness each term
- Pupil education integrated into curriculum (Digital Learning, PSHE/RSE)
- Staff Digital Device Policy signed by all staff
- Pupil Agreement read to Key Stage 1 and then read and signed by all children Year 3 – 6
- Data protection measures in place (encryption, password security)
- Incident reporting procedures followed for misuse or safeguarding concerns

PRINCE'S MEAD

Contents

Prince's Mead School aims to provide a safe environment to learn and work, including when online. Usage of digital devices including filtering and monitoring are important parts of the school's safeguarding arrangements, and it is vital that all staff understand the expectations, applicable roles and responsibilities in relation to this.

Staff, pupils, parents and visitors should be aware that the school's safeguarding systems apply to all users, all school owned devices and any device connected to the school's internet server.

1. Purpose & Principles

- To safeguard pupils, staff and the wider community in all online contexts (in-school and at home).
- Apply the same safeguarding standards online as offline; e-safety is integral to child protection.
- Teach pupils to **recognise, avoid and report online risks** (including but not limited to: bullying, grooming, abuse, radicalisation, identity theft).
- Embed critical thinking, digital citizenship and respectful conduct across the curriculum.

2. Scope

- Applies to all staff, pupils, parents/carers, governors, volunteers and visitors who access school IT or networks.
- Covers school-owned devices and personal devices used on site or on school networks (including Chromebooks, tablets, smartphones).
- Relates to on-site and remote/at-home learning activities where school systems are used.

3. Roles & Responsibilities

Governing Body

- Approve this policy annually and oversee effectiveness.
- Assure training for staff includes e-safety, filtering, and monitoring.

Headteacher & SLT & Head of Digital Learning

- Ensure appropriate filtering/monitoring; document decisions and reviews.
- Resource training; respond to escalations; ensure compliance is evidenced.

Designated Safeguarding Lead (DSL) &Head of Digital Learning

- Lead online safeguarding; respond to incidents; coordinate actions and records.
- Review filtering/monitoring reports and follow up on concerns promptly.

- Regular updates to staff and parents on emerging risks and how to report concerns.

Head of Digital Learning (Mrs Saffi Mant)

- Day-to-day coordination of e-safety practice and staff support.
- Liaise with IT and DSL on alerts, classroom needs and curriculum integration.
- Offer annual information evenings; practical home filtering/controls; conversation starters.

IT Staff

- Maintain secure infrastructure; operate filtering/monitoring systems; manage alerts.
- Conduct termly effectiveness checks; log and remedy issues.

All Staff

- Model safe practice; supervise use; follow Digital Device usage policy and safeguarding procedures.
- Report concerns immediately to DSL; record incidents accurately (preferably on CPOMS).

Pupils

- Pupils must follow the Pupil Agreement at all times and report any concerns to a trusted adult.
- Pupils may share work and collaborate using SharePoint, Purple Mash class folders, or Seesaw where appropriate.
- These platforms allow open sharing within the class, and enable staff to monitor work and view edits to support learning and online safety.
- Pupils must protect personal information and behave respectfully and responsibly online at all times.

Parents/Carers

- Support safe use at home; engage with school guidance and briefings.
- Share concerns with school; reinforce respectful and lawful online conduct.

4. Filtering & Monitoring

Please see Appendix 1 for more information.

- Applies to all users on school devices and to any device on school Wi-Fi; Chromebook use at home is also monitored.
- All internet traffic on the school network is filtered through the sonic wall hardware firewall. This also monitors malware and viruses.
- Whilst using the school network, a second filtering system (DNS filter) acts as a additional layer of protection. At home, pupils' chromebooks are protected by the DNS filter only.

All categories on the DNS filter are disallowed, and only sites that are approved onto the whitelist are accessible.

- Teaching exceptions may be requested via the Head of Digital Learning, IT department and DSL; decisions are recorded via the 'whitelist'
- Blocks harmful content (as stated in KCSiE guidance, see appendix 2); also restricts categories such as social media, gaming, gambling.
- Termly checks by IT; periodic reviews by DSL/Online Safety Governor; actions recorded.
- Impero ContentKeeper alerts go to HoDL and DSL simultaneously; concerns triaged and acted upon.
- Deliberate attempts to bypass controls are sanctioned under Behaviour/Staff Code of Conduct.

5. Education, Training & Curriculum

Staff (induction + annual updates)

- Roles/responsibilities for filtering & monitoring; reporting routes and thresholds.
- Recognising online risks (4Cs outline in KCSiE: content, contact, conduct, commerce) and early indicators.
- Termly update on safeguarding
- Annual Safeguarding training.

Pupils (progressive, age-appropriate)

- Y3: passwords; spotting misinformation; respectful communication.
- Y4: risk recognition; healthy screen habits; privacy basics.
- Y5: impact of sharing; digital footprint; peer responsibility.
- Y6: long-term consequences; bystander intervention; help-seeking pathways.

6. Devices & Acceptable Use

- Staff: use school devices for work; keep devices locked; delete pupil images/videos taken on personal devices the same day.
- Pupils: Digital devices are for enhancing learning tasks; non-school use is prohibited during the school day; misuse is sanctioned per Behaviour Policy.
- Reasonable adjustments: agreed with Learning Support/Matron for medical/SEND use of personal tech; teachers informed of arrangements.
- Booking of shared devices via Head of Digital Learning; staff sign devices in/out and supervise use.
- All devices are password protected.
- Year 1 have a specific Year 1 password and devices grouped.

- Ipads only work on an app bases.
- Year 3 have been allocated a number device from the Digital learning room to use every time.

7. Communications & Social Media

- Staff communicate professionally via school systems; no personal emails, numbers or messaging with pupils/recent alumni (<18).
- Pupils use school email for schoolwork; email and network activity are monitored; spam/malware protections in place.
- Social media: staff avoid personal social media during contact time; do not add pupils; protect confidentiality and reputation.
- Any offensive, discriminatory, threatening or bullying communication must be reported immediately to DSL; do not engage.

8. Data Protection, Security & Passwords

- Store data on school devices/SharePoint; encrypt removable media; avoid personal storage for school data.
- Strong, unique passwords; do not write down or share; change on schedule; simpler age-appropriate passwords used in Pre-Prep.
- Be vigilant for phishing/scams; report suspected breaches immediately to IT/DSL; follow incident response steps.

9. Digital Images & Consent

- Teach permanence and risks of sharing; avoid posting personal images publicly.
- Staff must seek approval from Marketing before publishing any online content and ensure parental consent requirements are met.
- Use images for legitimate educational purposes; store securely; delete when no longer required.

10. Artificial Intelligence (AI)

Staff may use **Microsoft Copilot** as this is protected within our school network and ensures that data is not shared externally. Approved uses include, but are not limited to:

- Proofreading and improving the clarity of written work
- Supporting the structure and drafting of reports
- Adapting and defining work for pupils with SEND

- Drafting letters and general communications

When using AI tools, **confidential information must never be entered**. This includes pupil data, staff details, parent information, or any other sensitive material. All AI-generated content should be treated as a draft only and must be carefully checked, edited, and verified by staff before use.

Staff must not seek or provide medical, health, or personal advice via AI tools. Any concerns of this nature should be directed to trusted professional sources or the DSL, in line with safeguarding procedures.

At present, staff must not use any other AI platforms for school-related work unless all personal and identifying information has been completely removed. This includes pupil names, staff names, and the name of the school.

Staff are responsible for ensuring that their use of AI complies with data protection requirements, safeguarding expectations, and professional standards at all times.

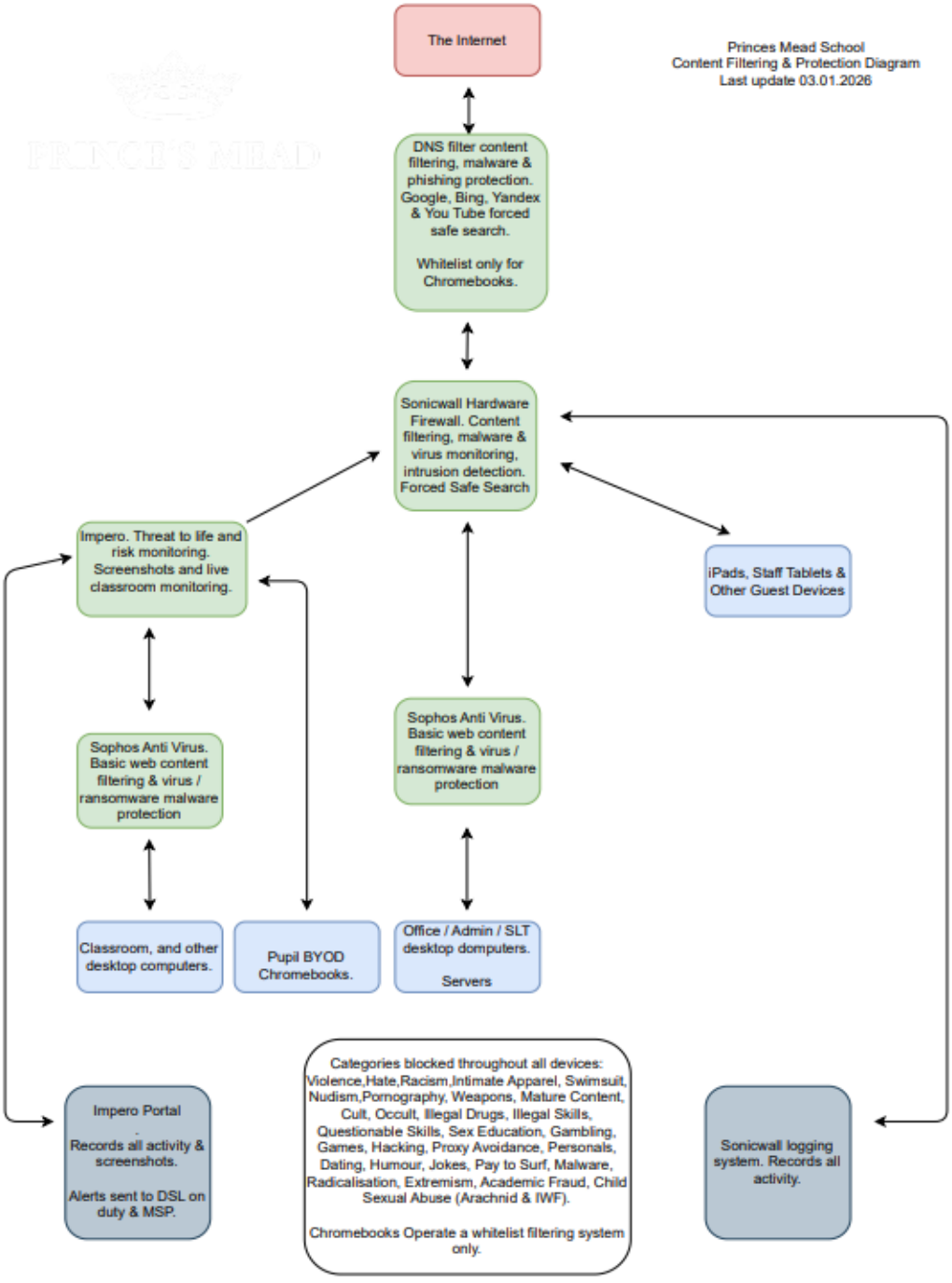
11. Misuse, Reporting & Complaints

- Illegal or harmful online activity may be referred to police/CEOP and safeguarding partners.
- Incidents recorded per Safeguarding & Child Protection Policy; immediate reporting to DSL.
- Complaints follow the Complaints Policy; outcomes and actions documented.

Linked Policies

- Safeguarding & Child Protection (incl. Prevent)
- Staff Code of Conduct
- Behaviour Policy
- Data Protection Policy & Privacy Notices
- PSHE/RSE Policy
- School Trips Policy
- Staff Digital Device Policy
- Pupil Agreement Policy

Appendix 1


The Internet
Princes Mead School
Content Filtering & Protection Diagram
Last update 03.01.2026
DNS filter content filtering, malware & phishing protection. Google, Bing, Yandex & You Tube forced safe search.
Whitelist only for Chromebooks.
Sonicwall Hardware Firewall. Content filtering, malware & virus monitoring, intrusion detection. Forced Safe Search
Impero. Threat to life and risk monitoring. Screenshots and live classroom monitoring.
iPads, Staff Tablets & Other Guest Devices
Sophos Anti Virus. Basic web content filtering & virus / ransomware malware protection
Sophos Anti Virus. Basic web content filtering & virus / ransomware malware protection
Classroom, and other desktop computers.
Pupil BYOD Chromebooks.
Office / Admin / SLT desktop domputers.
Servers
Impero Portal
Records all activity & screenshots.
Alerts sent to DSL on duty & MSP.
Categories blocked throughout all devices: Violence,Hate,Racism,Intimate Apparel, Swimsuit, Nudism,Pornography, Weapons, Mature Content, Cult, Occult, Illegal Drugs, Illegal Skills, Questionable Skills, Sex Education, Gambling, Games, Hacking, Proxy Avoidance, Personals, Dating, Humour, Jokes, Pay to Surf, Malware, Radicalisation, Extremism, Academic Fraud, Child Sexual Abuse (Arachnid & IWF).
Chromebooks Operate a whitelist filtering system only.
Sonicwall logging system. Records all activity.

Appendix 2 - Harmful Content Explained

In the 2025 guidance update, harmful content explicitly includes, but is not limited to, the following:

- Illegal Content: Child sexual abuse material (CSAM), content encouraging terrorism, and illegal, non-consensual sharing of intimate images.
- Pornographic Content: Explicit material that is not age-appropriate.
- Self-Harm and Suicide: Content that promotes, encourages, or provides instructions for self-harm or suicide.
- Violent Content: Material promoting extreme violence, serious injury, or, as of 2025, realistic depictions of violence.
- Bullying and Harassment: Content designed to bully, harass, or humiliate others.
- Hate Speech: Material inciting hatred based on race, religion, sex, sexual orientation, disability, or gender reassignment.
- Eating Disorders: Content that encourages or provides instructions for eating disorders.
- Radicalisation and Extremism: Content that promotes extremist ideologies.
- Misinformation and Disinformation: Fake news, conspiracy theories, and inaccurate information intended to deceive or harm, specifically added to the 2025 KCSiE guidance.
- Dangerous Challenges: Content encouraging stunts likely to cause serious injury.

Key Contextual Factors in KCSiE

- Impact over Legality: Content does not have to be illegal to be considered "harmful"; it just needs to cause distress or harm.
- Age Appropriateness: Content might be harmful because it is not appropriate for a child's age or maturity level.
- Filtering and Monitoring: Schools are required to have robust, tested systems to block this content.
- AI Risks: KCSiE 2025 explicitly mentions risks from AI-generated, synthetic, or manipulated content.