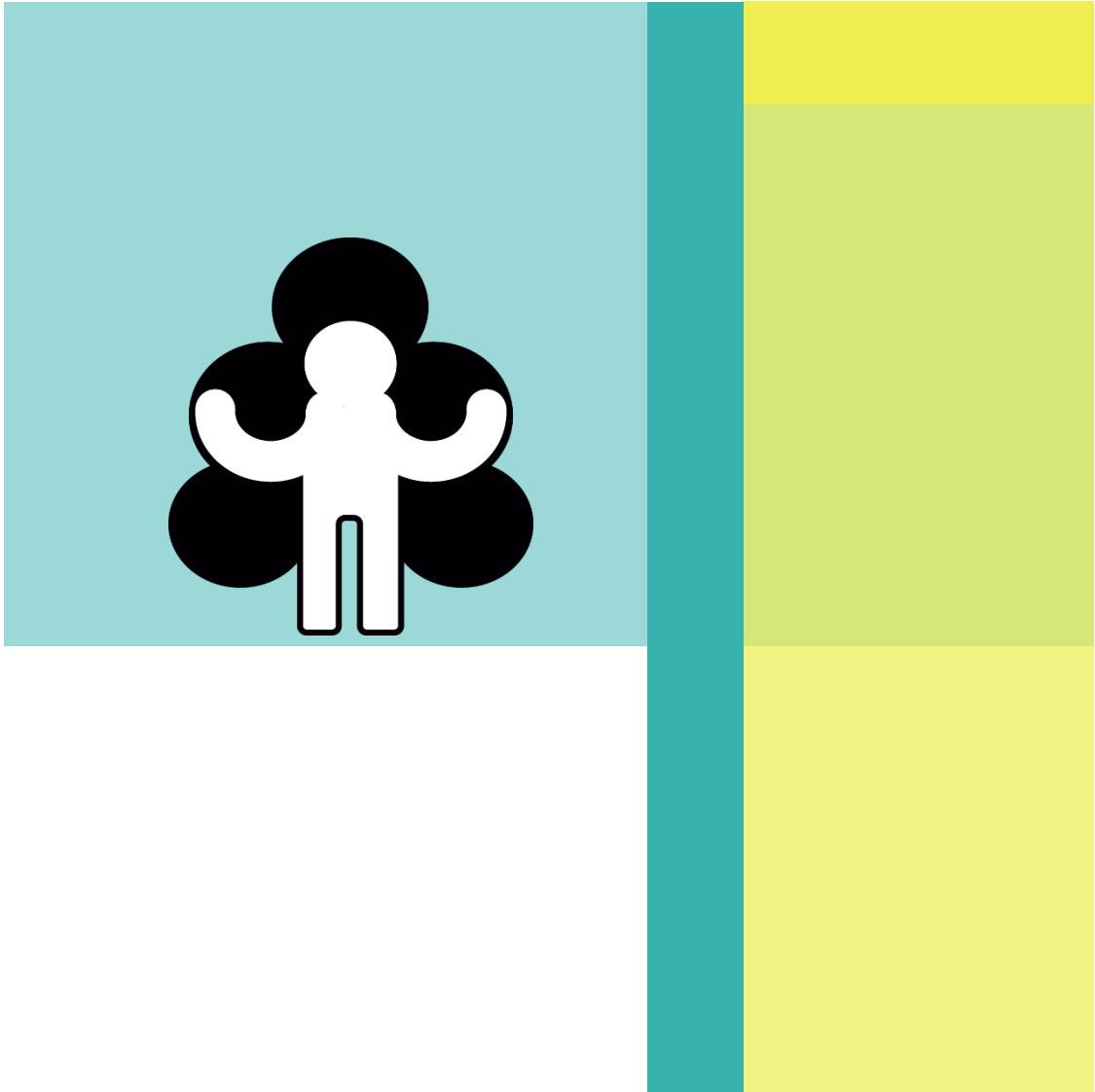


Ashmead School



Online Safety Policy

This policy was introduced on date: 01/01/26

This Policy will be reviewed annually and is therefore due for review in Oct 2027

1. Vision and Scope

At Ashmead Combined School, we recognize that technology plays an integral role in education and daily life. Our goal is to empower pupils aged 5 to 11 to become critical, responsible, and safe digital citizens.

This policy applies to all staff, pupils, governors, volunteers, and visitors who access the school network, internet infrastructure, or school-owned devices.

2. Roles & Responsibilities

Role	Key Responsibilities
Headteacher & Governors	Ensure online safety is embedded in overall safeguarding; review annual policy and audit technical controls.
DSL / Online Safety Lead	Manage incidents, maintain incident logs, liaison with external agencies, and coordinate staff training.
Network Administrator / IT Support	Maintain technical infrastructure, ensure Lightspeed Filter configurations remain up-to-date, and manage user access logs.
Teaching & Support Staff	Supervise pupil technology use, deliver age-appropriate online safety curriculum, and model safe behaviors.
Pupils	Follow acceptable use rules, respect peers online, and tell an adult immediately if something makes them uncomfortable.

3. Technical Infrastructure & Web Filtering (Lightspeed Filter)

To protect pupils from harmful online content while allowing access to valuable educational material, the school utilizes **Lightspeed Filter** across all school-issued devices (managed chromebooks, tablets, PCs) and internal Wi-Fi networks.

3.1 Filtering Standards & Controls

- **Real-Time Web Filtering:** Lightspeed Filter uses AI and smart database categorization to block inappropriate, adult, radical, or harmful content in real time.

- **SSL / HTTPS Inspection:** Lightspeed decrypts and inspects HTTPS content to ensure harmful search queries or media embedded in secured sites are blocked.
- **Age-Differentiated Profiles:**
 - **Early Years & Key Stage 1 (Ages 5–7):** Highly restricted access profile. White-listed or strictly vetted educational domains only; search functionality strictly controlled.
 - **Key Stage 2 (Ages 7–11):** Broader access to curated educational tools, video platforms (restricted mode), and search engines.
- **SafeSearch Enforcement:** Forced SafeSearch rules on Google, Bing, and YouTube for all school accounts and devices.

3.2 Real-Time Alerting & Monitoring

- **Alerting Keywords:** Lightspeed's safety engine actively monitors search queries and web visits for flags relating to self-harm, violent extremism, cyberbullying, or explicit content.
- **Escalation Path:** High-risk alerts generated by Lightspeed trigger an immediate automated email notification to the Headteacher and DSL for rapid review and intervention.

4. Curriculum & Digital Literacy

Online safety is taught regularly through the Computing curriculum, PSHE (Personal, Social, Health, and Economic education) for which the school uses JIGSAW, and dedicated national events (e.g., *Safer Internet Day*).

4.1 Key Stage 1 (Ages 5–7)

- Understanding how to ask a trusted adult for help when using technology.
- Keeping personal information private (names, passwords, photos).
- Recognizing that people online may be strangers.
- Practicing polite and kind behaviour in digital environments.

4.2 Key Stage 2 (Ages 7–11)

- Evaluating the reliability and trustworthiness of information found online.
- Understanding cyberbullying, its impact, and how to report it.
- Managing digital footprints and understanding privacy settings.
- Recognizing online risks, including grooming, inappropriate contact, and gaming risks (in-app purchases, open voice chats).

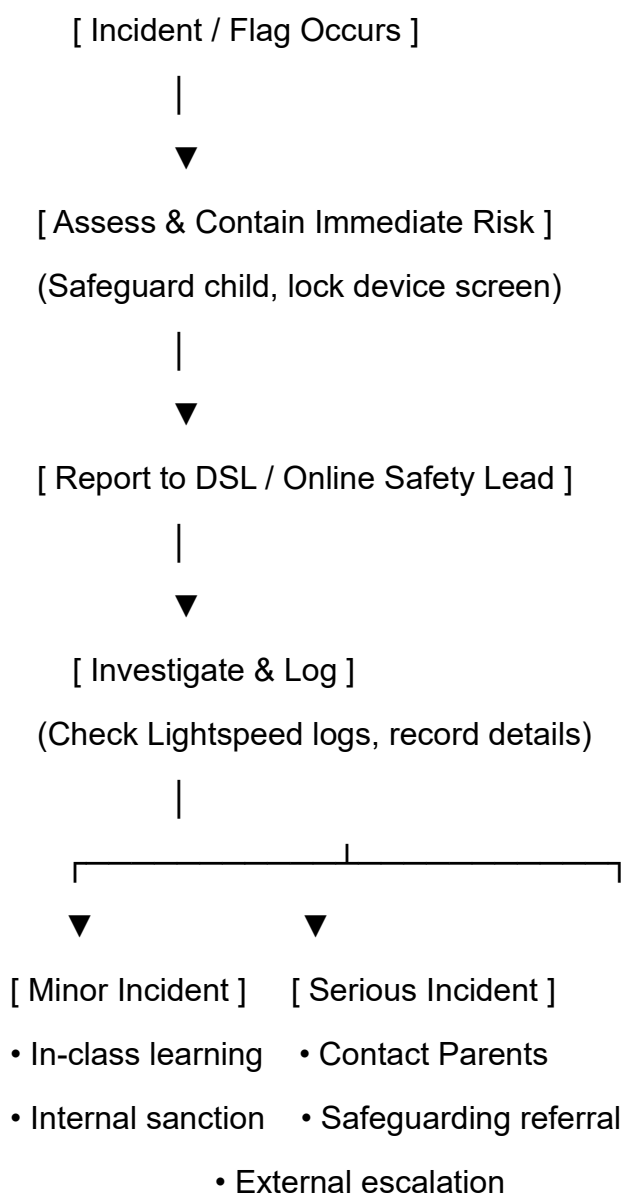
5. Pupil Code of Conduct & Acceptable Use Rules

We share simple, age-appropriate rules with pupils:

1. **Ask First:** Always ask an adult before using a device or going on the internet.
2. **Be Kind:** Use polite language and be a good friend online.
3. **Keep it Secret:** Never share full names, addresses, or passwords online.
4. **Report It:** Tell a teacher or trusted adult straight away if something feels wrong, scary, or strange.
5. **Protect Devices:** Handle school iPads, laptops, and computers with care.

6. Incident Management & Reporting

When an online safety violation occurs (or a Lightspeed flag triggers an investigation):



1. **Log Entry:** All incidents are logged in the school's central safeguarding database (CPOMS) with accompanying Lightspeed log reports where applicable.
2. **Parental Engagement:** Parents/carers are informed if a child is involved in a serious online safety breach or if concerns arise regarding search history.

7. Mobile Phones & Personal Devices

- **Pupil Devices:** Primary pupils are **not permitted** to use personal mobile phones or smartwatches with cellular connectivity during the school day. Any required phones (e.g., upper Key Stage 2 walking home independently) must be turned off and handed in to the class teacher upon arrival. Phones remain turned off and are returned to the pupil when they leave at the end of the day. Pupils are not permitted to use or turn phones on until they have left the school site.
- **Staff Devices:** Staff must not use personal devices or cameras to photograph pupils. Personal phones must remain in classroom cupboards, on silent at all times when pupils are in the classroom unless prior agreement has been sought from the Headteacher. Staff are permitted to use phones onsite during breaks and non-contact periods.

8. Policy Review & Training

- **Staff Training:** All staff receive annual safeguarding and online safety training, including awareness of emerging online trends and understanding how Lightspeed alerts operate.
- **Annual Audit:** The IAT facilities team and TurnItOn (the school and trust IT Management group) conduct an annual review of filter effectiveness. The Head Teacher and DSL conduct an annual review of incident logs, and policy updates.