

GDST
Filtering and Monitoring Policy
September 2026

Person(s) responsible for this policy		Assistant Head Pastoral	
Last review by	M.Furborough A.Nicholson	Review date	Sept 2026
Date of next review		September 2027	

Information

This procedure outlines our approach to filtering and monitoring internet content in order to comply with statutory requirements set out in "Keeping Children Safe in Education" (KCSIE) and the "Prevent Duty." Our goal is to ensure that our online filtering and monitoring provision effectively safeguards against harmful and illegal content, including child sexual abuse material (CSAM), and supports the well-being of our school community.

Every GDST student has an individual user account, which gives them access to Google Workspace for Education, Office 365, a range of learning platforms and the internet. Some students also have GDST-managed iPads or Chromebooks to support their learning.

To meet the standards set out in KCSIE the GDST use Lightspeed systems, which is an internet filtering solution that provides the ability to filter or block websites visited by users on any GDST managed device, whether on or off the GDST IT Network. The system also provides in depth monitoring, analysis and reporting on activity by users on all GDST managed devices (other than iPads). The system identifies when defined keywords are used or users have attempted at access blocked websites and provides this information in the system console/reports and generates notifications which are sent to the Designated Safeguarding Lead (DSL) when the system identifies patterns of behaviour that may indicate self-harm, violence, or bullying.

Duty of care to students

GDST devices and Internet access are provided to support our students' education and should only be provided where this supports their education.

Internet access should be disabled where this is in the interests of their wellbeing, and schools are asked to set overnight internet curfews, with times appropriate to each year group.

Parent Portal

Lightspeed Parent Portal is an application that gives parents visibility over their child's internet usage on school-issued devices.

Parent Portal allows parents to see websites accessed by students (including while at school), but not the search terms used, or activity on the site. Parents also receive a weekly email summarising web browsing activity, which they may opt out of.

Access to parent portal is determined by schools based on the parent email addresses provided to ServiceDesk@uk.gdst.net by their local IT team. Schools are free to decide who they enroll.

Filtering and monitoring

Filtering and monitoring are two components of online safety that work together to safeguard students.

Filtering blocks access to harmful or inappropriate websites and content, based on sets of rules applied to different categories of websites, whereas monitoring follows a user's activity and either generates flags when preset keywords are used, or generates alerts where the system identifies concerning behaviour.

How Lightspeed works with BYOD devices

BYOD devices are blocked from accessing the main GDST Network but are able to use our Guest Network.

When users sign into our Guest Network using their GDST credentials Lightspeed applies filtering categories appropriate to their role or key stage. Guest users without GDST credentials, or who do not sign in to their GDST browser have EYFS filtering rules applied.

Lightspeed uses a browser extension in the GDST Chrome and Edge browsers, which applies filtering and monitoring when a student is signed into their GDST browser, on any internet network.

Lightspeed also connects directly to Google Workspace for Education and Microsoft 365 to monitor student activity on these platforms.

How Lightspeed works with GDST devices

Lightspeed uses a browser extension in the GDST Chrome and Edge browsers, which applies filtering and monitoring when a student is signed into their GDST browser, on any internet network.

Lightspeed is installed as an agent on GDST managed Windows and iPads*, which provides comprehensive monitoring and filtering.

**Many apps (e.g. Safari, Chrome, YouTube) rely on web traffic which passes through the Lightspeed agent on iPads, and this is monitored by Lightspeed however some apps (WhatsApp, iMessage, Snapchat) use end-to-end encryption, and this content cannot be inspected by Lightspeed).*

Lightspeed also connects directly to Google Workspace for Education and Microsoft 365 to monitor student activity on these platforms.

Lightspeed filters

Websites are blocked or allowed, on or off the GDST IT Network for all users and devices according to predetermined rules. Different rules are set for staff, and students according to key stage

Information concerning websites that have been blocked or visited is displayed in the LightSpeed system console/reports (notifications are not sent). Logs are retained for 90 days.

Lightspeed monitoring

Flagged Terms are generated based on the use of pre-defined keywords. Where a pre-defined keyword is used a Flag is displayed in the LightSpeed system console/reports (notifications are not sent)

Lightspeed Alert provides an additional layer of safeguarding and combines the use of agents installed on devices (other than iPads), browser extensions, and integrations with Google and MS365, together with AI and contextual analysis to identify and automatically generate notifications for high-risk alert categories that include bullying, explicit language, drugs, self-harm, and violence.

Lightspeed alert with Human review is an additional service where a team of specialist at Lightspeed review the notifications generated by Lightspeed Alert, close any false positives, conduct a risk assessment, and then email any high-risk alerts to an escalation list, containing the contact details of nominated staff at the school and Trust Office. In the event of an imminent threat of harm to a student, the Human review team will also telephone staff on the school escalation list, then the Trust Office list, until they speak to a member of staff.

What do we need to respond to

Flagged Terms

The significant volume of keywords flagged by Lightspeed will be false positives, and the GDST subscribes to Lightspeed Alert which is a more sophisticated safeguarding tool. Flagged terms are visible to DSLs in their lightspeed dashboard however DSLs are NOT expected to proactively monitor flagged terms.

Lightspeed Alert notifications

Lightspeed uses AI and contextual analysis to identify and automatically generate notifications for high-risk alert categories that include bullying, explicit language, drugs, self-harm, and violence. The GDST subscribes to Lightspeed alert with Human review which provides an additional layer of scrutiny to alerts generated by Lightspeed.

DSLs should TURN OFF system generated notifications and only respond to alerts that are escalated to schools by the Human review team

Lightspeed Alert with Human review

Lightspeed Alerts are assessed by trained Lightspeed Safety Specialists, who are trained in threat assessment and suicide prevention. They evaluate alerts flagged by Lightspeed AI and contextual analysis to determine if they represent high-risk or imminent threats

The Human Review Team will conduct a risk assessment based on different levels of concern by looking at the alert itself and any additional context from web history, emails, chats, and more. The Human Review Team will escalate incidents to schools where they believe there is an Imminent threat, or where they believe there is a high risk.

Responding to high-risk alerts

High-risk alerts are defined as incidents where the “Context indicates threat is present, but no imminent new harm has occurred or will occur in the future”. When considering what is reasonable for responding to high-risk alerts there are several factors to consider.

- Severity or nature of the alert – alerts indicating an imminent threat should be responded to more quickly than alerts assessed as high-risk.
- Time of alert – was the alert generated during working hours, the evening, or weekend?
- Availability of staff – has the alert been generated when staff are working?
- Context – are there any known safeguarding risks, or trigger events (bereavement, external incidents)

During school hours high-risk alerts should be dealt with by school DSL or pastoral staff.

During office hours in school holidays parents are responsible for the welfare of their children, and our responsibility is to share information with them if we come into possession of information that indicates their child may be at risk of harm. Schools should ensure appropriate staff are available to respond to high-risk alerts during school office hours in school holidays. This may include Trust Office staff.

During Evenings and weekends, including bank holidays we have no formal arrangements requiring staff to work outside of their contractual hours. Where a threat is present, but it is not imminent, Lightspeed monitoring will continue, and high-risk alerts should be responded to on the next school or working day.

Responding to imminent threats

An imminent threat is defined as an incident where “context indicates new harm is imminent and the school or first responders should take immediate action”. In the event of an imminent threat, it would be unreasonable to wait until the next working day to respond, as the context indicates a child is at immediate risk of harm.

The Lightspeed Human Review Team will telephone staff on the school escalation list, then the Trust Office list, until they speak to a member of staff.

Outside of school hours parents are responsible for the welfare of their children, and our responsibility is to share information with them if we come into possession of information that

indicates their child may be at risk of harm. In the event that a parent cannot be contacted to inform them of an imminent threat it may be appropriate to escalate the matter to the Police. Safeguarding our students will always be our priority.

Updating school contacts for lightspeed

The Lightspeed Human Review Team will escalate incidents to schools where they believe there is High risk or an Imminent threat.

High risk alerts will be sent by email to all of the contacts provided by schools in their escalation list.

In the event of an imminent threat, in addition to emailing the alert to all of the contacts in the school escalation list, the Human Review Team will telephone the contacts in the school escalation list in order until they make contact with a member of staff, so it is important that schools provide contact numbers for staff members, not just a switchboard number.

The [school escalation list](#) can be found here.