GDST

GIRLS' DAY SCHOOL TRUST

GDST Filtering and Monitoring Procedure

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.

To meet these standards The GDST use Lightspeed relay, 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.

Lightspeed filtering and monitoring capability

Websites visited (all GDST managed devices)

- 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
- A number of categories of high-risk websites are blocked at a Trust wide level for all staff and students, however schools can define local rules for medium or low risk categories of websites.
- Information concerning websites visited is displayed in the LightSpeed system console/reports (Notifications are not sent). Logs are retained for 90 days.

Flagged Terms (not iPads, iPhones, MacBook *)

- These are generated by a client installed on each device based on pre-defined keywords.
- A default set of keywords is used by LightSpeed; however additional keywords may be added to the system
- Flags are displayed in the LightSpeed system console/reports (Notifications are not sent)

Safety Check (not iPads, iPhones, MacBook *)

- Lightspeed monitors student activity on school devices, uses advanced AI to identify students at risk, then send a notification to the DSL where it identifies on activity that is indicative of self-harm or other dangers.
- The notification includes a screen shot of the activity generating the alert.
- In order to generate alerts, a Chrome extension must be installed on the device. This is installed automatically when a user is on the GDST network, and they sign into their GDST google account

**These limitations are due to restrictions within the IOS and OSX operating systems*

BYOD Filtering and Monitoring

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 have EYFS filtering rules applied.

Lightspeed Notifications

GDST managed Laptop or Chromebook

- When users use flagged terms or attempt to access a blocked website this information is available to DSL's via the system console/reports. In addition,
- Lightspeed notifies the DSL when the system generates a safety check. GDST managed iPads, iPhones, MacBook
- Lightspeed makes information available to the DSL via the Lightspeed console when users attempt to access a blocked website

BYOD devices

- Lightspeed makes information available to the DSL via the Lightspeed console when users attempt to access a blocked website

Roles and Responsibilities

DSLs are responsible for reviewing and responding to notifications or alerts generated by Lightspeed where these indicate a safeguarding concern regardless of where and when they occur.

Safety check notifications that are false positives, or do not meet the threshold of a safeguarding concern may be closed in the LightSpeed console. Any online activity that indicates a safeguarding concern must be recorded on CPOMS and dealt with in line with GDST *Safeguarding Policy* and *Procedures*.

Responding to Notifications or Alerts

The standard expectation is that DSLs will review and respond to notifications or alerts during school hours.

KCSIE advises "It is a matter for individual schools and colleges and the designated safeguarding lead to arrange adequate and appropriate cover arrangements for any out of hours/out of term activities". Schools are free to conduct their own risk assessment and put additional cover in place to review or respond to alerts beyond school hours in response to sudden or local events if they consider this is appropriate.

While this risk assessment a is a matter for schools to decide, the following table provides some considerations

Standard risk (Minimum expectation)	DSL's will review and respond to alerts during school hours,
Medium risk Enhanced provision at the discretion of schools	regular daily checks with frequency of checks determined by the risk assessment (for example, every morning and afternoon)
High risk Enhanced provision at the discretion of schools	Cover determined by the risk assessment.

Note: The DSL community will be asked to further discuss monitoring during school holidays at the next DSL conference in September 2023 – Further guidance will then be issued

The timescales for responding to and dealing with notifications or alerts is not defined within statutory requirements, however guidance has been sought from a representative group of DSLs from across the GDST. The following table provides the agreed recommended responses and timescales for responding to alerts and flags generated by Lightspeed.

Lightspeed output	Appropriate response
Safety Check notifications are AI driven and a screen shot is provided showing the activity that generated the notification	• All safety checks notifications must be reviewed regardless of when they occurred. The target for this is within two school hours of the alert. • Reports will be graded by DSLs or a deputy using their professional judgement.

	• False positives may be closed in the lightspeed console with no further action
High risk Notification or report	Owned by DSL's, action needs to be taken within 24hrs of the report being reviewed • Export report as pdf • Add to CPOMS • Take action in line with *Safeguarding Policy/Procedures*.
Moderate risk Notification or report	DSLs may assign to another member of staff, action needs to be taken within 72hrs of the report being reviewed • Export report as pdf • Add to CPOMS • Assign to a member of staff to take action in line with *Safeguarding Policy/Procedures*
Low risk Notification or report	DSLs may assign to another member of staff, action needs to be taken within 1 week of the report being reviewed • Export report as pdf • Add to CPOMS • Assign to a member of staff to take action in line with *Safeguarding Policy/Procedures*.