Addendum to the staff, pupil and volunteer privacy notices for schools using **eSafe**

Schools have a statutory duty to monitor their digital environment in order to identify any potential threats to pupil's welfare and wellbeing.
At Langer Primary Academy and in our secondary schools (including Churchill and Sir Bobby Robson) this monitoring is carried out by eSafe.
eSafe combines intelligent detection software, expert human behaviour analysis and dynamic threat libraries to identify a range of safeguarding risks.

All school owned devices will be continuously monitored for safeguarding risks. If pupils and staff use a school owned device outside of school, the device will continue to be monitored when it is both online and offline.

A Data Protection Impact Assessment (DPIA) has been completed for eSafe. Below is an addendum to the staff, pupil and volunteer privacy notices.

The purposes for processing	To monitor user's activity in the digital environment, provided by the school, in order to detect and alert markers of risk to safety, welfare and wellbeing.
The lawful basis for processing	Schools are legally required to comply with statutory obligations regarding safeguarding and child protection. As such, schools may rely on article 6 (1) (c) of the GDPR (General Data Protection Regulation): processing is necessary for compliance with a legal obligation to which the controller is subject. (The Prevent Duty and the Department for Education's statutory guidance: Keeping Children Safe in Education)

And

Schedule 1, Part 2, Paragraph 18 of the Data Protection Act 2018, processing special category data for the purpose of safeguarding children and individuals at risk. |
The categories of personal data obtained	• User login ID • Date and time stamp of when an incident occurs • ID of the device in use • Screenshot of the user's screen at the moment the incident occurred, details of attempts to access potentially illegal content • Information about a user's health (including mental health such as self-harm/suicide risk) • Information about a user's political opinions where there is a suspicion that those opinions may be extreme or concerning.
The recipients of the personal data	In certain circumstances, when we have a cause for concern, we may share your personal data with police forces, the NHS or local authorities (e.g. social care).
The retention periods for the personal data	eSafe will retain screenshots and reports for six months from the date of an incident. The retention by schools of screenshots and/or reports provided by eSafe for the purpose of investigating concerns is covered in the trust's record retention policy
Your rights	Your rights over your personal data are unaffected and are as stated in the pupil, staff and volunteer privacy notices

How the service works

eSafe

1 A User logs on

2 An alert is triggered

3 The incident is examined by a Behaviour Analyst

4 They determine if it's genuine or not
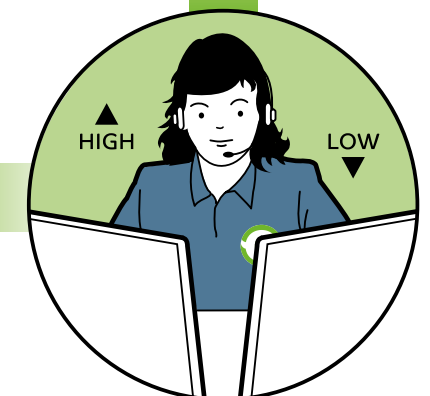
Key to incident categories

A Illegal, life threatening

B Serious e.g. bullying, mental health, racism, pornography

C Less serious e.g. profanities, vulgarities

7 **Category B** incidents are reported that day by email

Category C incidents are detailed in a weekly round-up report, by email

6 **Category A** incidents are reported immediately by telephone, and within a report that is emailed the same day

5 Genuine incidents are assigned a threat level

See key to incident categories opposite

HIGH ▲   LOW ▼

esafeglobal.com