Privacy notice – Filtering and Monitoring School Systems

Our internet and online systems are used to support teaching and learning, pastoral and wellbeing, financial and personnel issues.

To do this we have to be mindful that staff, pupils, volunteers, and visitors may access the internet to undertake tasks.

We have an obligation to put in place suitable Filtering and Monitoring systems, these will apply to our devices used on site, and for devices used offsite where proxy is deployed. Filtering and Monitoring will also apply to personal devices that access our internet connection on the site.

Filtering is the safety measure designed to restrict and control the content which can be accessed by staff, pupils, volunteers, and visitors.

Monitoring concerns the review of user activity on the school's network to promote the safeguarding of staff, pupils, volunteers, and visitors.

Management of Data

We will use third party systems to manage the Filtering and Monitoring obligations that are Department for Education requirements and are set out in Keeping Children Safe in Education and are part of the wider safeguarding standards that are mandatory.

The records will be retained for 2 years. However, there may be instances where elements need to be retained for a longer period if there are safeguarding concerns.

This data will be processed as part of a Public Task with a Legal Duty to implement the systems and procedures.

What do we do with the data?

The data will be reviewed internally by suitably appointed Safeguarding and IT professionals. There may be occasions when it is necessary to share material with third parties such as the police, social care or health professionals. Sometimes this can be done without any notification to the person or person who have been the source of the concerns.

If matters need to be raised with individuals this will be done according to our wider data protection, safeguarding and employee policies as is appropriate.

What will it be used for

The data will be used to monitor internet activity where a user has attempted, either deliberately or inadvertently, to access potentially inappropriate or harmful website content which has been blocked by our filtering systems. The data will be used to identify an individual to enable the appropriate follow-up support or action if it is felt appropriate by the Designated Safeguarding Lead at the school.

How long will we keep it

The reports will be kept for no longer than 2 years unless the data has been used to support a significant safeguarding concern. In this case the report may be retained in line with the recommended timeframe according to the nature of the concern.

How will we store it
Reports are received via MS365 email which is encrypted in transit and protected by delegated user access, these will be automatically deleted from the email server after a period of 2 years. Any reports that are required to support an ongoing concern will be saved to a secure document area with permissions restricted to only those persons with responsibility for managing the concern.

Will it be shared with others
Designated Safeguarding Leads may share this information with the Head Teacher and nominated Director for safeguarding at the Trust. Information will only be shared with third parties such as the police, health or social care services where it is deemed necessary.

Your data protection rights
For more information about how data is collected, stored, used, and protected, please see our data protection policy which can be found on our website.

You will find details about your rights and how to access data we hold, and what to do is you are not satisfied or wish to complain.