BELPER SCHOOL
and Sixth Form Centre

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, whether used on site or off site. Filtering and Monitoring will also apply to personal devices that access out 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 12 months. 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 I necessary to share material with third partiers 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

IT staff receive alerts when search terms on any of the block lists are detected. IT Staff use their judgement as to whether the alert is a safeguarding concern based on experience of student behaviour and context. They then pass any relevant information to the school safeguarding team for follow up with the user concerned.

How long will we keep it

The provider retains data for 12 months.

How will we store it

The data is stored on the Surfprotect servers in Exa Networks datacenter. Data is accessed via a secure web portal using a username and password only known to IT Support staff. Alerts with basic information are emailed to IT support staff for further investigation.

Will it be shared with others

Relevant information may be shared with others if appropriate and within safeguarding and GDPR guidelines.

If so, who

The school safeguarding team to follow up on concerns. School staff to notify of potentially unwanted activity during lessons. Other agencies permitted with safeguarding and GDPR guidelines.

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.