Privacy Notice for Filtering and Monitoring

Success Academy Trust (registered office Thomas Estley Community College, Station Road, Broughton Astley, Leicestershire, LE9 6PT) is the Data Controller for the purposes of the Data Protection Act 2018 and General Data Protection Regulations 2018 (GDPR). Guided by these acts, we offer protection for individuals, but share data when it is required by law or is beneficial to the individual. Under data protection law, individuals have a right to be informed about how the Trust and its schools uses any personal data that we hold about them.

For the contact details of the local school Data Protection Manager (DPM) or the Trust Data Protection Officer (DPO) please see our Data Protection page on www.successat.org.uk.

1.0 Scope/overview

This privacy notice covers all Academies/schools within Success Academy Trust.

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.

2.0 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 in line with our Records Retention and Disposal Schedule policy. 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.

3.0 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.

4.0 What will it be used for?

- To identify risks
- To enable early interventions
- To promote responsible cyber use

- To protect pupils from online dangers
- To raise awareness of the need to be safe

5.0 How long will we keep it?

Information will be stored in line with our Records Retention and Disposal Schedule.

6.0 How will we store it?

RM Web Filter - Administrators can produce browsing reports for any five-day period within the last 12 months from the admin console, if further reports are required a support call would need to be logged with our third line provider. RM Safety Net partners in India with strict security and data protection procedures following ISO 27001 best practice.

Classroom Cloud E-safety/ Net Support - Data is retained for 13 months if the account is still in subscription, if the subscription does lapse the data is held for 30 days before being deleted. Records can be exported as a CSV or printed at any time before the 13-month limit or the 30-day limit.

Cloud Server Backups – Our third line IT support provider's local NAS backup 2 months Cloud backup of servers and data is for 12 months if still in subscription if the subscription does lapse the data is held for 30 days before being deleted.

Office 365 data held on Microsoft servers are GDPR compliant with EU ISO 27001 safe harbour.

7.0 Will it be shared with others?

Access shared with DSL, SLT and the Network Manager as appropriate.

8.0 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 Trust website. Successat.org.uk

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.