



SchoolPro DPO
Leadership Capacity

The Latest Data Protection Hot Topics

Data Sharing, Subject Access, Biometrics, Generative AI, and DUAA

Who are SchoolPro TLC?



Data Protection



Health & Safety



Attendance



SEND



**Curriculum &
Timetabling**



Safeguarding



Data Analytics

The Latest Data Protection Hot Topics

Guidance for Data Sharing with School Immunisation Services



Discover the latest DfE guidance on data sharing for school immunisation programmes. Learn how schools and trusts can lawfully share data with SAIS teams under UK GDPR, ensuring compliance and supporting public health initiatives. Read more for actionable advice and key steps for school leaders.

Updated Subject Access Request Guidance for MATs & Schools



Discover how the latest DfE guidance on Subject Access Requests (SARs) can reduce your school's administrative workload. Learn key updates, practical tips, and how to ensure compliance with updated tools and policies.

Guidance on Biometric Data for MATs and Schools



Stay informed with the latest guidance from the Information Commissioner's Office (ICO) on the use of biometric data in schools and multi-academy trusts (MATs). This blog outlines the legal obligations, consent requirements, and best practices for safeguarding student and staff biometric information. Learn how to comply with UK GDPR, conduct Data Protection Impact Assessments (DPIAs), and implement secure biometric systems, while ensuring transparency and ethical use. Perfect for school leaders and data protection officers looking to protect personal data effectively.

Guidance on the use of Generative AI in MATs and Schools



With great power comes great responsibility! The use of Artificial Intelligence (AI) in schools is rapidly growing, offering numerous benefits such as enhanced efficiency, personalised learning, and improved decision-making. However, AI also presents challenges, including data protection risks, ethical considerations, the risk of bias, and concerns over transparency. Given the rapid advancements in AI and [...]

Principle 1 - Data Sharing

It is important to know what your lawful bases are for:

- § Processing Data, and
- § Sharing Data

Legal Bases for Data Sharing

- § **Public Task** - necessary for a task carried out in the public interest
- § **Legal Obligation** - necessary to comply with a legal obligation
- § **Vital Interest** - necessary to protect vital interests
- § **Legitimate Interest** - necessary for the purposes of legitimate interests for the controller *or* a third party
- § **Performance of a Contract** - necessary for the performance of a contract to which the data subject is a party
- § **Consent**

Data Sharing Example:

- § Schools must provide certain data to School Age Immunisation Service (SAIS) teams to support immunisation efforts.
- § Providing a list of eligible children and young people, along with their parents' or carers' contact details
- § The sharing of contact details **does not equate to consent for immunisation.**

Data Sharing Example:

- § The guidance confirms that sharing this data is lawful under Article 6(1)(e) of the UK GDPR.
- § **Sharing data with immunisation teams is in the public interest.**
- § Supporting public health initiatives falls under the school's official authority.



Topic 2 - Biometric Data 🙌

What is Biometric Data?

- § Personal information is only biometric data if it:
 - § relates to someone's physical, physiological, or behavioural characteristics (e.g. the way someone types, a person's voice, fingerprints, or face);
 - § has been processed using specific technologies (e.g. an audio recording of someone talking is analysed with specific software to detect qualities like tone, pitch, accents, and inflections); and
 - § can uniquely identify (recognise) the person it relates to.

Consents for Biometric Data

- § Protection of Freedoms Act 2012 - governs the use of biometric data in schools
- § The consent of **at least one parent** is required to process the biometric data **of a child under 18**
- § If the child or any parent objects, the school cannot process the child's biometric data.

Who Can Consent?

- § Schools must notify each parent.
- § Provided no one objects (parent or child), written consent of only one parent will be required.
- § The child does not have to object in writing.
- § Parent's objection must be in writing.

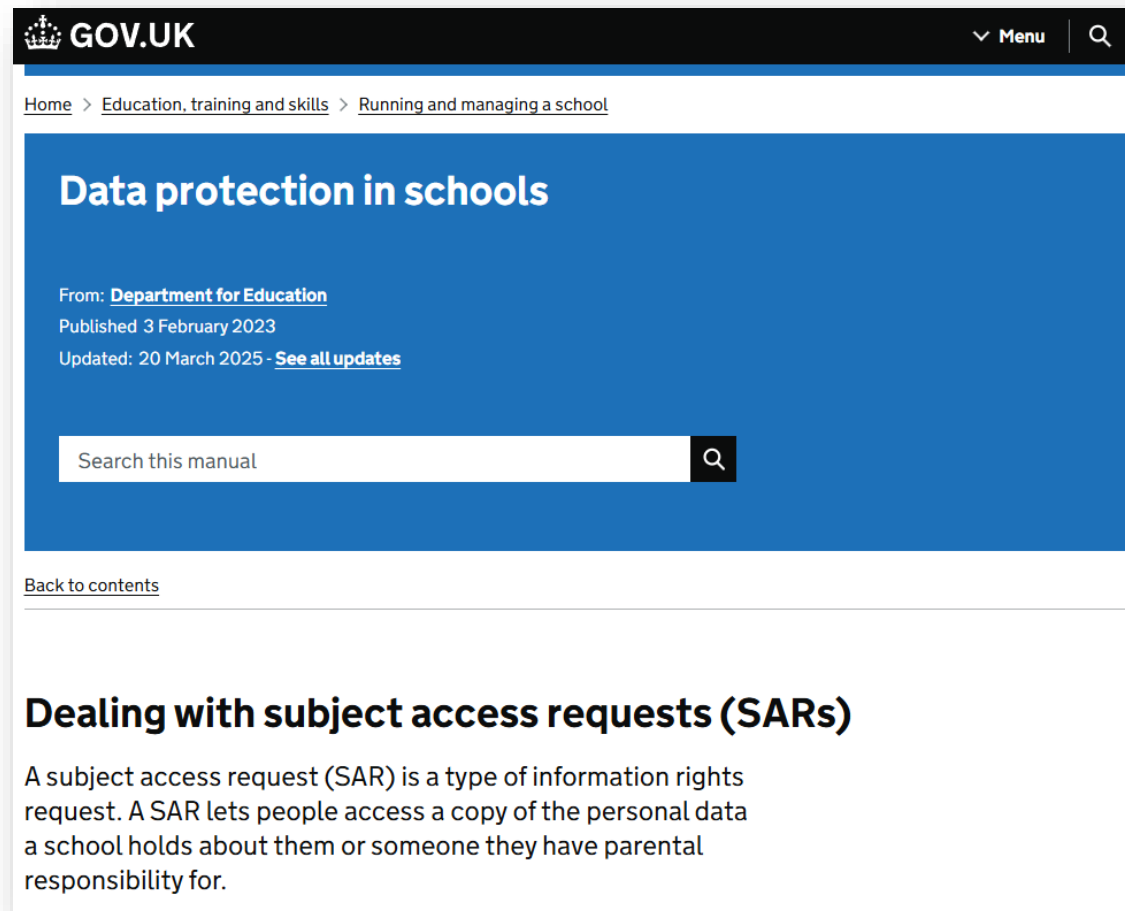
Third Party Contractors

- § Ensure that they comply with data protection laws.
- § Ensure that due diligence checks and appropriate risk assessments (DPIAs) are in place.
- § Ensure that appropriate security measures are in place.
- § Ensure third-party contractor staff have had:
 - § data protection training;
 - § training on the biometric system; and
 - § an understanding of key processes regarding consent.

Actions for Schools and MATs

- § Conduct a Data Protection Impact Assessment (DPIA)
- § Obtain Proper Consent
- § Be Transparent with Parents and Students
- § Implement Robust Security Measures
- § Choose Vendors Carefully
- § Ensure Appropriate Processes and Training are in Place

Topic 3 - Subject Access Requests



GOV.UK Menu

[Home](#) > [Education, training and skills](#) > [Running and managing a school](#)

Data protection in schools

From: [Department for Education](#)
Published 3 February 2023
Updated: 20 March 2025 - [See all updates](#)

Search this manual

[Back to contents](#)

Dealing with subject access requests (SARs)

A subject access request (SAR) is a type of information rights request. A SAR lets people access a copy of the personal data a school holds about them or someone they have parental responsibility for.

Updated DfE Guidance

Dealing with information already held by the requester

“If a requester already has information previously provided by the school or has access to information, you do not need to resend this in your response. You will still need to explain that you hold that information and explain why you are not releasing it.”

How Does This Save Time?

Here's a practical example:

A parent submits a SAR requesting copies of their child's academic progress.

If the school has already provided the same data through a parent portal or during a previous request, you can acknowledge the data's existence and explain that it won't be reissued.

By avoiding duplication, you can focus on new elements of the request, reducing workload.

Next Steps for Schools

Review your SAR process

Make sure that everyone is aware of the updated guidance and how to apply it.

Update your documents

Ensure that the updated guidance is reflected in relevant policies and privacy notices.

Communicate clearly

Ensure data subjects are aware of their rights and your approach to SARs.

What Else to Understand about SARs?

- § Understand what exemptions can apply and when
- § Understand what to redact and how
- § Understand when extensions can be applied to SARs
- § Understand the scope of a SAR - only **personal data**

Topic 4 - Generative AI

Guidance on the use of Generative AI in MATs and Schools

by Soton Soleye & Ben Craig | 03 Mar 2025



The use of Artificial Intelligence (AI) in schools is rapidly growing, offering numerous benefits such as enhanced efficiency, personalised learning, and improved decision-making. However, AI also presents challenges, including data protection risks, ethical considerations, the risk of bias, and concerns over transparency. Given the rapid advancements in AI and the growing reliance on these technologies in education, it is crucial for MATs and schools to establish clear policies that balance innovation with safeguarding concerns.

This guidance provides a framework for the responsible use of AI in schools, ensuring compliance with UK GDPR, recommendations from the Information Commissioner's Office (ICO), the Department for Education (DfE), and guidance from Ofsted.

What is Generative AI?

- § AI systems that can create new content such as text, images, video or audio
- § Content is created using machine learning to create original outputs from input data
- § Defined as mimicking cognitive functions associated with human intelligence

General AI Best Practices

- § Verify all AI-generated content for accuracy before use
- § Use AI tools to enhance learning and reduce workload, not to replace professional judgment
- § Stick to school-approved AI tools that comply with data protection policies
- § Maintain human oversight - never rely solely on AI for assessments or decisions
- § Be transparent - let students and staff know when AI has been used in content creation
- § Train staff and pupils on AI's risks, limitations, and ethical considerations

Open vs Closed AI Systems

§ Open

- § Often publicly available, these learn continuously from user inputs
- § May store, share or learn from information entered

§ Closed

- § Generally controlled by the organisation using the system
- § Greater security and compliance as data inputs not accessed externally
- § Some Open systems can be configured as 'Closed' depending on their settings and environment when deployed

AI & Data Protection in Schools

- § Avoid Using Personal Data in AI Tools
- § Strictly Necessary Use
- § Transparency in Automated Decision-Making
- § Legal Basis for AI Data Processing
- § Security Measures

Ofsted Expectations for AI Use

- § Safety, Security and Robustness
- § Transparency
- § Fairness
- § Accountability
- § Contestability and Redress

DfE AI Guidance

Released June 10th 2025:

- § [AI revolution to give teachers more time with pupils - GOV.UK](#)
- § [Using AI in education: support for school and college leaders - GOV.UK](#)
- § [Using AI in education settings: support materials - GOV.UK](#)

And Finally...

- § Update policies, privacy notices, and acceptable use agreements (AUA) as needed.
- § Consult your Data Protection Officer (DPO) if in doubt.

Topic 5 - Data Use & Access Act 2025

- § Gained Royal Assent in June 2025
- § Phased implementation over 12 months to summer 2026
- § SARs - Reasonable and proportionate searches
- § Complaints Processes - statutory requirement for DP Complaints
- § New Lawful Basis - 'recognised' legitimate interests

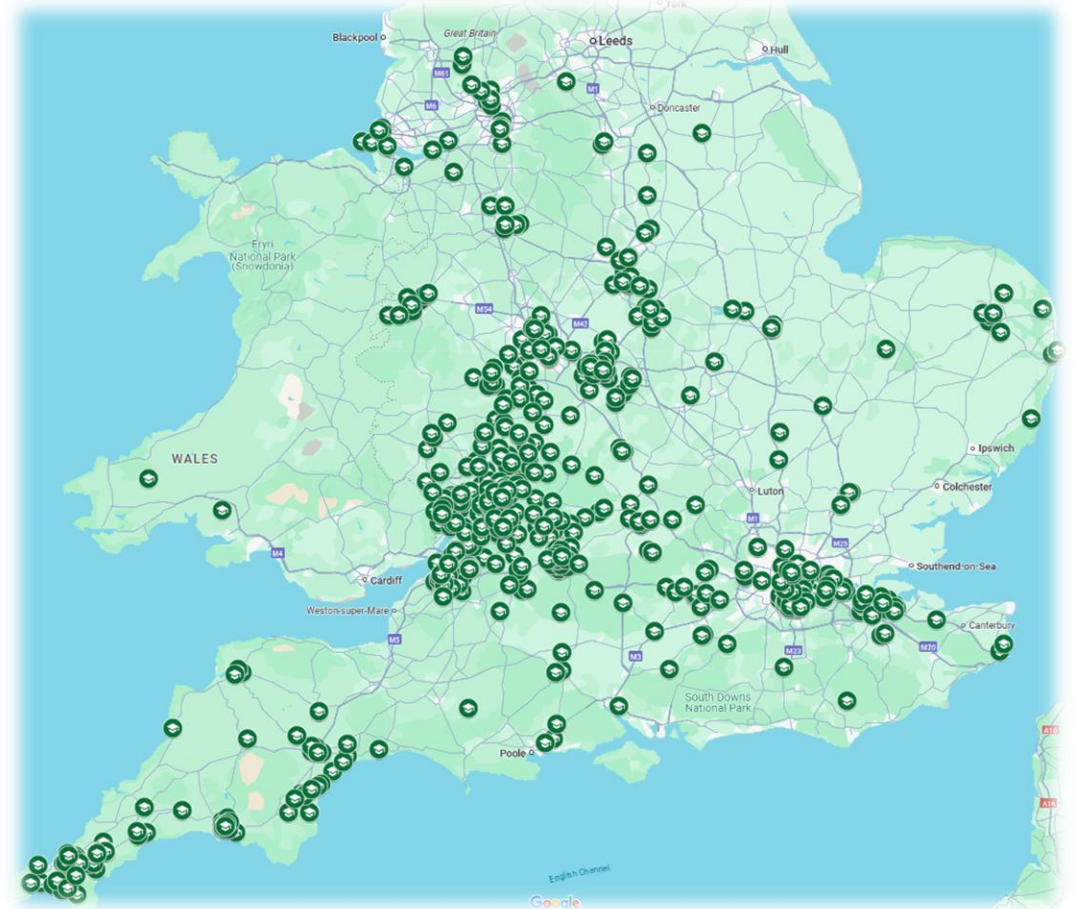
The Latest Data Protection Hot Topics

Ben Craig

DPO@schoolpro.uk

www.schoolpro.uk

@SchoolProTLC





SchoolPro TLC

Leadership Capacity