Saint Michael's CE High School

A Church of England Academy

Therefore, choose

General Data Protection Regulation Policy

Responsibility to present to Headteacher	CFO / Business Director
Approval	Finance, Premises, H&S Committee March 2026
Next Review	Finance, Premises, H&S Committee March 2027
Statutory	Yes
Required on school website	Not statutory – school decision to publish

ST MICHAEL'S CHURCH OF ENGLAND HIGH SCHOOL

A BRIEF SUMMARY OF OUR CHRISTIAN VISION

Our motto is **'Therefore choose [life]'** from Deuteronomy.

We understand this to mean growing in **body, mind and spirit**, so that all who learn and work here may flourish, experiencing the joy and hope of

'Life in all its fullness'.

This is further explained in our Mission Statement,

'As a vibrant learning community
we choose to serve God,
pursue excellence
and celebrate the uniqueness of each individual.'

Contents

What data protection means for schools

Data protection practices ensure that an organisation and the individuals within it can be trusted to collect, store and use personal data fairly, safely and lawfully. Information contained within this policy, follow the DfE guidance data protection in schools.

This advice is intended for maintained schools and academies

- understand how to comply with data protection law
- develop their data policies and processes
- know what staff and pupil data to keep
- follow good practices for preventing personal data breaches

Data protection legislation, and who and what it's intended to protect.

Good data protection practices ensure that an organisation and the individuals within it can be trusted to collect, store and use our personal data fairly, safely and lawfully.

All those who process others' personal data have to follow strict rules.These rules are set primarily by:

- the UK General Data Protection Regulation (UK GDPR)
- the Data Protection Act 2018 (DPA)

The Data Use and Access Act 2025

The Data Use and Access Act is a new Act of Parliament. It changes data protection laws to promote innovation and economic growth. DfE will provide further information on what these changes mean for the education sector in due course.

Data Processing a school is permitted to do

Personal data

Personal data is information that relates to an identified or identifiable living individual.

In a school, examples of personal data include:

- identity details (for example, a name, title or role)
- contact details (for example, an address or a telephone number)
- information about pupil behaviour and attendance
- assessment and exam results
- staff recruitment information
- staff contracts
- staff development reviews
- staff and pupil references

Under UK General Data Protection Regulation (UK GDPR), there are 6 lawful bases on which personal data is permitted to be processed. You need to ensure at least one lawful basis for processing applies and identify which of the 6 bases is the most appropriate.

The lawful bases are:

- **consent** – where this basis is the most appropriate and you're able to give the individual concerned a real choice in your use of their data
- **contract** – where your use of the data is necessary for a contract the school has or will have with the individual concerned
- **legal obligation** – where your use of the data is necessary to permit the school to comply with the law
- **vital interests** – where your use of the data is necessary to protect an individual's life

- **public interest** – where your use of the data is necessary to permit the school to carry out a task in the public interest or its official functions, and that task or function has a clear basis in law
- **legitimate interests** – where your use of the data is necessary for the school's or a third party's legitimate interests (unless there's a good reason to protect the individual's personal data that overrides those legitimate interests)

You can read the Information Commissioner's Office (ICO) guidance on the lawful basis for processing personal data.

Special category data

Special category data is personal data that's considered more sensitive and given greater protection in law.

Special category data includes:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade-union membership
- genetic information
- biometric information (for example, a fingerprint)
- health matters (for example, medical information)
- sexual matters or sexual orientation

In a school, it would be best practice to also treat as special category data any personal data about:

- a safeguarding matter
- pupils in receipt of pupil premium
- pupils with special educational needs and disability (SEND)
- children in need (CIN)
- children looked after by a local authority (CLA)

Under UK GDPR, there are 10 additional conditions for processing special category data. You need to ensure that at least one lawful basis and one condition – which does not have to be linked to the lawful basis – applies.

The conditions are:

- **explicit consent** – the accessing or processing of this personal data has the written consent of the individual concerned
- **employment, social security or social protection** – it's necessary for one of these 3 stated purposes and authorised by law
- **vital interests** – it's necessary to protect an individual's life
- **not-for-profit body** – it's necessary for the legitimate internal-only purposes of a membership body with a political, philosophical, religious or trade-union aim
- **manifestly made public** – it relates to personal data the individual has themselves deliberately made public
- **legal claims or judicial acts** – it's necessary for a legal case or required by a court of law
- **substantial public interest** – there's a relevant basis in UK law and one of 23 specific public interest conditions has been met
- **health or social care** – it's necessary for the provision of healthcare or treatment, or of social care, and there's a basis in law
- **public health** – it's necessary for reasons of public interest, and there's a basis in law

- **archiving, research and statistics** – it's necessary for reasons of public interest, and there's a basis in law

The Data Protection Act 2018 (DPA), Schedule 1, Parts 1 and 2 has more information about the conditions that are authorised or have a basis in law and the further actions that might be necessary to permit you to process certain personal data.

You can read the ICO's guidance on the lawful basis for processing special category data.

Personal data breaches

A data breach is a security incident that results in personal data a school holds being:

- lost or stolen
- destroyed without consent
- changed without consent
- accessed by someone without permission

Data breaches can be deliberate or accidental. A breach is about more than just losing personal data. Use the ICO's lawful basis interactive guidance tool to help you decide whether you have the legal right to process particular personal data items and on what grounds.

Criminal offence data.

Criminal offence data is personal data that's treated in a similarly sensitive way to special category data. It records criminal convictions and offences or related security measures.

Criminal offence data includes:

- the alleged committing of an offence
- the legal proceedings for an offence that was committed or alleged to have been committed, including sentencing

Schools process criminal offence data in storing the outcome of a Disclosure and Barring Service (DBS) check on their employees, non-employed staff and volunteers. As this data relates to criminal convictions, collecting and retaining it means the school is processing criminal offence data. This applies even though the check has not revealed any conviction.

You can read about handling DBS data in the statutory guidance on keeping children safe in education.

Criminal offence data is treated in a similar way to special category data. One of the 6 lawful bases must apply and your processing must also be covered by one of the conditions described in Schedule 1 of the DPA.

You can read the ICO's guidance on the lawful basis for processing criminal offence data.

Assessing whether there's a condition to support the processing of special category or criminal offence data - and, if there is, which one is most applicable - is not always obvious.
The ICO offers further guidance on the lawful basis.

Lawful consent

When there is no legal obligation to process personal data for a particular purpose, it may be appropriate to obtain an individual's consent. If the lawful basis of **consent** applies, the condition for processing any special category data within would be **explicit consent** - that is, consent that has been confirmed in a written statement.

UK GDPR defines consent as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. For consent to be considered 'freely given', an individual must suffer no detriment if they refuse to give it.

Data Subjects

Schools collect, store and use personal data about a variety of individuals. In this context, those individuals are known as data subjects.

A school's data subjects include:

- pupils and former pupils
- parents and carers
- employees and non-employed staff
- governors and trustees
- local-authority personnel
- volunteers, visitors and applicants

Data Assets

Schools hold personal data in several forms. These are collectively known as its data assets.

- data items – single pieces of information
- data item groups – data items about the same process
- data sets – collections of related data that can be manipulated as a unit by a computer
- systems – administrative software
- system groups – the larger systems housing administrative software

The Data Use and Access Act is a new Act of Parliament. I changes data protection laws to promoted innovation and economic growth. DfE will provide further information on what this means to schools in due course.

Responsibilities

Who is responsible for making sure data is processed securely in a school.

Everyone in your school is responsible for protecting personal data. There are some key roles and responsibilities for data protection compliance.

The data controller

For most of the personal data you collect, store and use, the school or the multi-academy trust is the data controller. This means it's responsible under the Data Protection Act 2018 for protecting data in every situation where it decides:

- whose information to collect
- what types of data it needs
- why it needs it
- whether the information can be shared with a third party
- when and where data subjects' rights apply
- for how long to keep the data

As a data controller, your school needs to register with the Information Commissioner's Office.

Where, for example, a school is required to supply a copy of some personal data to the Department for Education (DfE), DfE also becomes an independent data controller of the copy it receives.

Governors and trustees

The responsibility and accountability for compliance sits with governors and trustees. Schools and multi-academy trusts risk getting a fine if they don't comply.

Governors and trustees check that the school:

- monitors their data protection performance
- supports the data protection officer
- has good network security infrastructure to keep personal data protected
- has a business continuity plan in place that includes cyber security

Academy trusts: governance guide - GOV.UK provides essential information from a range of sources on the trust board's roles and legal responsibilities.

Senior leaders

Senior leaders are accountable for:

- deciding how the school uses technology and maintains its security
- deciding what data is shared and how
- setting school policies for the use of data and technology
- understanding what UK GDPR and the Data Protection Act covers and getting advice from the data protection officer, as appropriate
- assuring governors and trustees that the school has the right policies and procedures in place
- making sure any contracts with third-party data processors cover the relevant areas of data protection
- making sure staff receive training on data protection every 2 years (we recommend annually as best practice)

Staff training on data protection should include training on specific school processes such as:

- personal data breach reporting processes
- the escalation of information rights requests

All staff

All staff should be aware of what:

- personal data is
- 'processing' means
- their duties are in handling personal information
- the processes are for using personal information
- is permitted usage of that data
- the risks are if data gets into the wrong hands
- their responsibilities are when recognising and responding to a personal data breach
- the process is for recognising and escalating information rights requestsThis includes:
- teaching staff
- catering staff
- welfare supervisors
- library staff
- cleaners
- first-aiders
- governors and trustees
- volunteers

There are extra requirements for any staff in school who:

- create and store data
- enter data into applications or software
- decide if and when they'll process certain data
- handle paper documents

Staff who collect, store or view personal data are responsible for:

- making sure they have a legitimate need to process the data
- checking that any data they store is needed to carry out necessary tasks
- identifying any risks
- understanding the governance arrangements that oversee the management of risks

Staff are responsible for making sure that pupils using personal data for projects or coursework do so appropriately. This includes being compliant when storing data. The Information Commissioner's Office has guidance on training for staff. It also produces resources to help you promote good data protection practice in your school.

Role of data protection officers

How data protection officers can help make sure schools are compliant with data protection laws. All maintained schools and academies must have a designated data protection officer. A data protection officer can cover more than one school.

Data protection officer's responsibilities

The data protection officer in your school is responsible for:

- advising school leaders and staff about their data obligations
- monitoring compliance
- conducting regular data audits
- developing and updating data protection policies and procedures
- monitoring who in the school has access to personal data
- advising when data protection impact assessments are needed
- answering data protection enquiries from staff, parents and pupils
- making sure privacy notices are regularly reviewed and updated
- supporting and advising staff who have data protection queries
- communicating with the Information Commissioner's Office (ICO)
- reporting to the governing board or trustees about data protection
- advising the governing board or trustees on data protection risks
- advising on and co-ordinating responses to information rights requests
- making sure all assets containing personal data are appropriately managed and secure

Appointing your data protection officer

You have different options for appointing your data protection officer or data protection lead. You could:

- re-align responsibilities in your current team
- share the data protection officer role between a group of schools
- ask for volunteers within the wider school community
- consider procuring a contracted service

Your data protection officer needs to be impartial. Any other duties they perform should:

- be compatible with their duties as a data protection officer
- not lead to a conflict of interest

Training, knowledge and skills

Your data protection officer should know about:

- data protection
- UK GDPR
- the way your school operates
- the technology and systems you use
- cyber security

The data protection officer role includes a significant level of responsibility. You should make sure they have the appropriate time, resources and support to carry out the role effectively.

Data protection policies and procedure

Under UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA), schools have to:

- comply with the legislation
- demonstrate that they're complying

You can read more about the personal data you need to document and how to do so on the Information Commissioner's Office (ICO) website, where there is a useful data controller's checklist.

Statutory policies

It's a legal requirement that your school has data protection policies and procedures in place and that you regularly review and update these, along with the associated documentation. You should also review the statutory policy for maintained schools or the statutory policy for academy trusts in the light of data protection legislation.

Record of processing activities

A record of processing activities is an efficient means of capturing all the important information about your school's data processing activities. It will improve your information governance and show your compliance with accountability principles. It will also ensure you comply with other aspects of data protection law, such as the requirement to create privacy notices and keep data assets secure, thereby reducing the risk of a personal data breach. Guidance on how to document your processing activities is available on the ICO website.

Step 1: identify your personal data assets

Locate all the personal data your school has received, created or shared. It could be stored in:

- management information systems
- communication systems
- safeguarding technology
- health and social care records systems
- curriculum management software
- virtual learning environments
- workforce systems
- catering systems
- equipment records
- photo and video storage systems
- paper records and photos
- statutory returns to the Department for Education (DfE) and local authorities

Step 2: list your personal data assets

Compile a list of that personal data. Start with broad data item groups, then add beneath each group specific data items. For example, the data item groups for pupils might be:

- admissions
- attainment
- attendance
- behaviour
- exclusions
- personal identifiers, contacts and pupil characteristics
- identity management and authentication
- catering and free school meal management
- trips and activities
- medical information and administration

- safeguarding and special educational needs

Repeat this for the personal data assets of all data subjects in the school community.

Step 3: add information about your personal data assets

Record extra detail about each of the personal data items in the list. There's no definitive format you need to follow in creating your record of processing activities, so develop your own to suit your school's needs, using this guidance as a starting point.

Mandatory information

Your record of processing activities should include the following as a minimum:

- the name and contact details of your school
- the name and contact details of your data protection officer (DPO)/data protection lead
- the name and contact details of any joint controllers
- the purposes of the personal data processing you carry out
- the categories of personal data you process
- the categories of individuals whose personal data you process
- the categories of organisations with which you share personal data
- the schedule for retaining each category of personal data
- a general description of your technical and organisational security measures

Additional information

The following prompts will help you add more detail about each personal data item to your record of processing activities.

Source of personal data

Record whether the data item:

- was received by the school
- was created by the school
- has been or will be shared by the school

Category of personal data

Record whether it's:

- personal data
- special category data
- criminal offence data

Data controller or data processor

Record whether, in respect of this data item:

- the school's a data controller or a data processor
- the school's a joint controller and, if so, with which organisation
- there's an up-to-date controller-processor contract in place, if applicable

Access and use

Record, in respect of this data item:

- the lawful basis (personal data) and, if applicable, additional condition (special category or criminal offence data) that allows it to be accessed and used
- who has access to it and how that's controlled
- whether there's an up-to-date data sharing agreement in place, if applicable

Data retention and destruction

Record, in respect of this data item, the:

- data retention period and the justification for it
- procedure for depersonalisation or disposal of it at the end of the retention period
- disposal is manual or automated and, if manual, there's a prompt to ensure it is destroyed

Consent, rights and subject access requests

Record whether, in respect of this data item, data subjects have:

- given their consent for it to be processed and, if so, how
- been informed of their rights regarding access, rectification and erasure
- been told about the procedure for making a subject access request

Security and personal data breaches

Record whether, in respect of this data item, there:

- are up-to-date information and communication technology (ICT) security policies and procedures in place to prevent a cyberattack
- is a procedure for secure sharing
- is a procedure for handle a personal data breach

Automated decision-making

Record whether, in respect of this data item, the processing involves any automated decision-making. Share your record of processing activities with your school leadership team (SLT) and governors or trustees. They are responsible for ensuring your school is compliant with the DPA and keeps only the personal data it needs.

Data Protection Impact Analysis (DPIA)

A DPIA is a tool to help you identify, measure and manage data protection risks. Under UK GDPR, a DPIA is needed whenever the processing of personal data is likely to result in a 'high risk to the rights and freedoms' of individuals.

An effective DPIA will help you:

- identify, manage and mitigate data protection risks
- fix problems at an early stage, minimising those risks
- consider and mitigate risks to individuals' privacy
- ensure individuals' expectations of privacy obligations are being met - for example, by the provision of privacy notices
- provide individuals with reassurance
- demonstrate both accountability and compliance with data protection law
- avoid reputational damage to your school

You should consider and document carrying out a DPIA of personal data collected:

- about vulnerable data subjects, including:
    - children (because of their age)
    - employees (because the power imbalance means they cannot easily consent or object to the processing of their data by an employer)
    - more vulnerable sectors of the population (who need special protection)
- by innovative technologies, such as:
    - biometrics
    - internet of things applications
    - safeguarding equipment, such as CCTV

Review your record of processing activities

Look again at each personal data item in your record of processing activities and ask yourself whether:

- there are any current data processing activities that do not have a lawful basis (personal data) and, if applicable, additional condition
- as the result of applying those justifications, you would be less likely to carry out any safeguarding activities – if so, re-assess how you're applying the law
- you're certain about the procedure for data sharing in every case, including when this takes place and with which organisations
- there's a procedure in place for updating the data sharing agreement with any organisation to which you're passing personal data
- there's a procedure in place for updating your ICT security policies, and regular training for everyone who handles personal data
- the school's systems allow you to carry out responsible data retention, depersonalisation and disposal procedures
- everyone in the school community knows the procedure for reacting to a personal data breach and that procedure has been tested

Record the risks

There's no definitive DPIA format you must follow, so you can develop your own to suit your school's needs, using this guidance and your own risk management framework as a starting point.

You can download a suggested DPIA template from the ICO website.

A DPIA does not have to demonstrate that all risks have been eliminated, but it'll help you document them and assess whether any that remain are justified.

If it identifies a high risk and you cannot take measures to minimise it, you'll need to seek advice from the ICO. You may not begin processing the personal data in question until you have acted on the ICO's advice.

Regularly reassess the impact

A DPIA is not a one-off exercise. You need to keep it under regular review and update it if anything changes in your school's data life cycle.

In particular, if you make any significant changes to how or why you process personal data, or the amount of personal data you collect, it has to demonstrate that you've assessed any new risks.

You should also review your DPIA if a new:

- security flaw is identified
- technology is made available
- contractor is appointed
- public concern is raised over the type of processing you do
- public concern is raised over the vulnerability of a particular group of data subjects

Privacy Notices

Under UK GDPR and the Data Protection Act 2018, every school must make its privacy notices freely available to those whose personal data it handles.

A privacy notice explains:

- why a school needs to collect personal data
- what it plans to do with it
- how long it will keep it
- whether it will be sharing it with any other organisation

Privacy notices need to be clear and accessible, and regularly reviewed and updated. Being transparent builds trust, avoids confusion and lets everyone in the school community know what to expect.

Privacy notices should be reviewed by your data protection officer:

- at least annually
- whenever you make a significant change to how you process personal data

Parents, pupils and staff, who are the data subjects , must be notified in the case of any significant changes to your privacy notices or if the way you use their personal data changes.

What to include in a privacy notice

Your privacy notice is expected to explain to your data subject what makes it lawful for the school to use personal data, including any data that may be regarded as sensitive. The Information Commissioner's Office (ICO) has a list of what a privacy notice should contain.

Your school's privacy notice must include what personal data your school shares with DfE.

Model privacy notices for schools to issue to staff, parents, carers and pupils about the collection of data are available.

A privacy notice can be in any format, provided it is accessible. For example, you can take a layered approach, where you provide a short version of your privacy notice, along with details of how to view further information.

Data subjects' rights

Data subjects have rights and control over the use of their personal data. These rights are:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing
- the right to data portability
- the right to object
- rights in relation to automated decision-making and profiling

Your privacy notice should include:

- what personal data is being processed
- why their personal data is being processed
- on what lawful basis their personal data is being processed
- with whom their personal data will be shared and why
- how and for how long their personal data will be stored
- how they can exercise their rights over their personal data
- whom to contact if they have any questions or concerns, including your data protection officer and the ICO

The information in your record of processing activities will be a useful source of information in this regard.

Inform data subjects about their privacy rights

Privacy notices are the most common way of complying with data subjects' right to be informed. There are a number of ways you can keep data subjects informed about how your school deals with their personal data.

For pupils, these include sharing the school's privacy notice:

- in an induction pack, when joining the school
- at the start of each school year
- when they provide extra personal data during the school year
- through the school website

For staff, these include:

- when they apply for a role, accept a contract, are appraised, or leave the school
- ensuring existing staff members are made aware of the privacy notice at the start of each school year
- making the notice visible on the staff notice board and intranet

For pupils and staff, you must make sure the privacy notice is accessible at all times.

Download this example template (MS Word document, 30KB) which offers a simple way for a school to seek parents' and carers' consent to process children's personal data at the same time as they ask them to confirm or amend it.

Children have the same rights over their personal data as adults. Schools can be inventive in the way they present child-friendly privacy rights information, using diagrams, graphics, comic strips, videos and so on. For example, DfE has a privacy notice specifically for children and young people. Introducing the idea of data privacy within wider online safety lessons will allow teachers to use age-appropriate language, ensure understanding and encourage pupils to ask questions.

Personal information shared with DfE

DfE collects personal information from educational settings, local authorities, and other organisations, via various statutory data collections. Each data collection or census guide contains the legislation detailing the lawful basis for collection.

This data is used for many purposes, including to inform funding, monitor education policy and school accountability, and to support research.

Your school's privacy notice must include what personal data is shared with DfE. You can read examples of this text in DfE's privacy notice model documents.

Cyber Security

It's essential to ensure critical data is protected from cyber-attacks and unauthorised access. You should be aware of what personal data you store within your school network, and what's stored outside of your direct control. Both locations must have in place good security settings, including encryption and access control, and all those processing personal data should be trained in keeping data safe.

DfE has guidance to help schools keep people and their personal data safe when using digital technology, and on meeting ICT service and equipment standards.

The government's National Cyber Security Centre has resources to improve cyber resilience.

They include:

- information about better protection in cyberspace
- device security guidance
- cloud security principles
- tools to strengthen cyber defence
- cyber security training for staff
- home learning technology advice
- data security tips

The police service's regional cyber protect officers provide free advice and training to schools.

Sharing personal data

Who you can share personal data with and what consent you need to get – for example, when publishing exam results, taking photos in school and for immunisation programmes.

To keep children and young people safe in school, you need to share information appropriately, so the correct decisions can be made to protect them.

You must have a compelling reason to share their personal data. Sharing children's data with third parties can expose them to unintended risks if not done properly. You should carry out a data protection impact assessment to assess any risk before sharing personal information about your pupils.

The Information Commissioner's Office website includes further guidance on data sharing. Any data you share must comply with their data sharing code of practice.

Safeguarding

To keep children safe and make sure they get the support they need, you can share information with other schools and children's social care teams. It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child.

Your designated safeguarding lead will decide if personal data needs to be shared. They should make sure they record:

- who they're sharing that information with
- why they're sharing the data
- whether they have consent from the pupil, parent or carer

Read working together to safeguard children to find out more information about sharing a pupil's safeguarding file. You should also refer to the safeguarding section of keeping children safe in education.

Sharing data with local authorities and government

Occasionally, you may need to share personal information about your pupils with local authorities, other schools or children's services. For example:

- if a pupil shows signs of physical or mental abuse, you may need to pass this information on to children's services
- another school may need to know which pupils will be at their sports day or on a joint school trip

Sharing information can help provide appropriate services that safeguard and promote the welfare of children. The Data Protection Act 2018 and UK GDPR provides a framework to make sure that personal information is shared appropriately.

Before you share any data, you must:

- consider all the legal implications
- check if you need permission to share the data
- confirm who needs the data, what data is needed and what they'll use it for
- make sure that you have the ability to share the specified data securely
- check that the actions cannot be completed or verified without the data

You also have a statutory requirement to share personal data about your pupils with DfE through the school census. You do not need to get consent from pupils, parents or carers to share this data with us. You should provide information about what data you share in your school's privacy notice. Privacy notice model documents suggest wording to explain to staff, parents, carers and pupils what data you're collecting and sharing. Schools may also need to share personal data about their staff with the local authority.

Sharing data with other schools

If a pupil moves to another school, you should transfer their records to the new school. This includes the pupil's common transfer file and educational record.

You must:

- make sure you transfer the data securely
- transfer the record within 15 days of getting confirmation the pupil is registered at another school
- be able to trace the record during the transfer

To securely share and transfer pupil records, you could:

- use the school to school (S2S) system
- send them to a named person using an encrypted email
- ask your local authority to transfer them
- deliver any paper records in person or ask the new school to collect them

If you're organising a school trip with another school, you'll need to share data with them to confirm which pupils are going. You may also need to share details such as dietary requirements or medical information to make sure pupils are safe. Where you already have consent for the information, make sure this also covers sharing it.

What you need consent for

Before sharing any personal data, you need to identify the lawful basis. This may be consent from the individual. There may be some circumstances where it may not be appropriate to ask for consent, however.

For example:

- if the individual cannot give consent
- it's not reasonable to ask for consent
- when there's a safeguarding concern

You'll usually need to get the pupil's consent to share their data if they're aged 13 or over. If they're under 13, you must get consent from whomever holds parental responsibility for the child. Guidance on understanding and dealing with issues relating to parental responsibility is also available. The Information Commissioner's Office has guidance to help you understand a child's rights over their personal data.

How to get consent

You can get consent in different ways. It must be clear that the individual agrees to share their personal data and understands what they're agreeing to. Do not use pre-ticked boxes or add disclaimers that state that, by not responding, they are agreeing to share their data.

You should keep a record of:

- the consent
- when you got the consent
- how you got the consent – for example, keeping the letter you sent to parents or carers

When getting consent, you need to explain:

- what personal information you're sharing
- why you're sharing it
- who you're sharing it with and what they'll use it for
- how you'll share their information
- the process for withdrawing consent

Any letters you send to parents or carers that ask for a reply slip that includes personal data should have a data protection statement. This could mean linking to a privacy notice or including information within the letter.

If you're asking for consent from a pupil aged 13 or over, you must write your request so they can understand it and are clear about what they're agreeing to. Download an example template for a letter to parents and carers about consent.

Ensuring data subjects have their rights respected when using biometric data

If you use pupils' biometric data as part of an automated biometric recognition system, such as using fingerprints to receive school meals instead of paying with cash, you must comply with the requirements of the Protection of Freedoms Act 2012.

That means following these steps.

1. In accordance with the child's age or capacity, get written consent from at least one parent or carer before you take and process any biometric data from their child. See the section on consent over age of 13.

2. Provide an alternative means to access the relevant services for any pupil from whom you do not have consent. For example, pupils must be able to pay for school meals using cash at each transaction, if they wish.

3. Delete any relevant data already captured, if a parent or carer withdraws their consent.

If a pupil does not want their biometric data processed, you must not process it even if their parent or carer has given consent. This is required by law.

You also need to get consent from any staff members using the school's biometric system. Staff can withdraw their consent at any time and you must then delete any relevant data already captured.

Guidance is available on protecting children's biometric information in school.

Taking and using photos in school

Photos are used in school for many different reasons. You'll need to identify the lawful basis for each different use of a photograph.

You should have a clear photo policy published alongside your privacy notice and provide copies of both to parents and carers.

You may be able to use photos in printed materials such as a prospectus or marketing materials under the lawful basis of legitimate interest. However, you need to provide pupils, parents or carers with an opportunity to object before you go to print.

You must get consent to share photos on your school's social media channels or elsewhere online.

If you're using a photo of a pupil, do not include their name unless you have specific consent to do so. You should only use a photo in line with the consent provided. When you're asking for consent, you should make it clear for how long you'll use the photograph.

Photos used in identity management systems may be essential for performing the public task of the school, but you should delete them once a child is no longer a pupil at your school. The Information Commissioner's Office provides further guidance on taking photos in school.

Download an example template for a letter to parents and carers about consent. This includes a section on taking and using photos of pupils in school.

Publishing exam results

UK GDPR does not stop schools from publishing exam results online or in the local press.

You do not need to get consent from pupils, parents or carers to publish exam results. However, you should tell pupils where and how their results will be published before they're published. This gives them an opportunity to ask you to remove their results from the list should they wish to.

The Information Commissioner's Office has more information about exam results and data protection.

School immunisation programmes

You will need to provide data to support immunisation programmes in your school. This includes:

- sharing information leaflets and consent forms with parents or carers
- providing a list of eligible children and young people, and their parent's or carer's contact details to the School Age Immunisation Service (SAIS) team

Sharing these contact details does not mean that a vaccine will be given. A parent or carer will need to give their consent for a vaccine to be given to their child.

There is a lawful basis for you to share information with school immunisation teams under article 6(1)(e) of UK GDPR. This states that the information can be shared if "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller ".

This means that the school can share this information with immunisation programmes as it is in the public interest. Sharing information with immunisation programmes is part of the exercise of a school's official authority. Schools also have a duty to support wider public health.

Data protection laws do not prevent you from sharing personal data where it is appropriate to do so in a fair and lawful way, and in this instance it is beneficial to do so.

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.

This guidance is for people working in the education sector who respond to subject access requests (SARs).

You can make it easier to respond to a SAR by:

- having good record keeping practices, including retention periods
- making parents and carers aware of how they can find personal data they already have access to
- keeping an accurate record of how you have dealt with a SAR

Receiving a SAR

Any individual whose personal data is held by an education setting can make a SAR. Personal data is information that relates to an identified or identifiable individual.

In this guidance the person making a SAR is referred to as the requester.

Individuals can ask for a SAR from anyone who works at an organisation. In a school this could include:

- teachers
- support staff
- school volunteers

Individuals can make a SAR in any format. They could make a verbal request, or a written request via a letter, text, or email. Once an individual has made a request, you cannot ask them to change the format they made the request in.

When an individual asks for their personal data, they do not have to call it a SAR. You will need to be aware that someone could be making a SAR if they:

- make a complaint
- quote other legislation, such as a freedom of information request

When working in an education setting you may receive a SAR from:

- students
- anyone with parental responsibility for a child (either for themselves or on behalf of the child)
- employees (such as teachers, classroom assistants and support staff)
- volunteers
- governors
- third parties, such as legal organisations, acting on behalf of another person

Information an individual can request

A requester can ask for any personal data that relates to:

- themselves
- someone they have parental responsibility for
- someone they have permission to act on behalf of

Encouraging requesters to self-serve

If the requester already has access to the information they want to see, you can direct them to this. For example, the requester may already have access to personal data stored on the school's website.

You do not have to treat this request as a SAR, provided they can access the information within one calendar month.

Responding to a request from a child

Requesting a SAR is a child's right. A child can request access to information about themselves from any education setting that holds data about them. A child does not have to be a certain age to make a SAR. The Information Commissioner's Office (ICO) provides guidance on the rights of children when making SARs.

If the young person is under 13 and is making their own request, you will need to consider whether they will be able to understand your response, but this shouldn't be a barrier to supplying them with their information.

If the young person is over 13, you should treat the request the same way as if an adult made it, provided there are no issues with the child's competency.

Parents or carers can also make a SAR on behalf of a young person. If the young person is 13 or over, check whether they are happy for their personal data to be shared with their parent or carer.

When a child of any age submits a SAR, you should assess if they can understand the information they will receive in response to their request.

If you believe the child has the maturity and understanding to request and receive the information, you should respond directly to the child, regardless of their age. If a child requests

a SAR themselves, this demonstrates some maturity and understanding about their right of access their personal information.

You should not respond directly to the child if you believe they:

- do not have the maturity or competence to act independently
- have a health condition that limits their understanding
- have given consent for a representative or someone with parental responsibility to act on their behalf

In these cases, contact the child and ask if they agree for their parent or carer to make the request on their behalf.

The ICO provides guidance on SARs from young people.

Ways someone can submit a SAR

A requester can submit a SAR:

- in writing, such as an email, letter, or via social media
- verbally, such as over the phone or face-to-face

It is the responsibility of the school to treat a request for information as a SAR.

The person requesting information does not need to refer to the process as a SAR.

For example, a parent could ask for a copy of an incident report, regarding their child, during a phone call with a school. As the parent has asked for personal data, the school should treat this request as a SAR.

You should not ask the requester to make a SAR in a different way once they have made their request. You can create a preferred request method, such as a standard form, but should not insist a requester makes a SAR in a particular way.

Timeframes for responding to a SAR

A full SAR response must be sent to the requester within one calendar month.

You can extend the SAR deadline if you have to wait for the requester to provide identification, authority and any clarification you might need. For example, if it takes 3 days for the requester to provide identification, you can extend the deadline by 3 days.

If the request is complex, the response time can be extended by up to a further 2 calendar months, making the response deadline 3 months in total. The ICO advise that you should respond to the SAR as soon as possible within the extended period.

For complex requests, you must tell the requester the new deadline and the reason their SAR is being treated as complex. You must do this in writing, within one calendar month of the original request date.

In most cases, having to retrieve or redact a lot of information does not make a SAR complex. It is up to individual schools to assess whether a SAR is complex.

The ICO provides guidance on complex requests.

Calculating how long you have to respond to a SAR

Organisations have one calendar month to respond to a SAR, starting from the day a SAR is submitted. If you receive a request on the last day of the month and the following month is shorter, a response must be made by the last day of the shorter month. If a SAR is received on 31 January, a response is required by 28 February (29 February in a leap year). If the deadline for a response falls on a weekend or bank holiday, you can respond on the next day. For example, the deadline for response is 2 May which is a bank holiday, the response deadline becomes 3 May.

Read more about SARs response times on the ICO website. There are online calculators that can help you work out how long you have to respond to a SAR.

Delays to SAR processing

In some cases, the calendar month response time can be paused if you are unable to progress with the request.

You may need to pause the request if:

- you are waiting for a requester to confirm their identification
- you are waiting for the requester to provide evidence of their authority to act on behalf of another individual
- you are seeking reasonable clarification about the request

Read more about delaying a SAR response on the ICO website.

Receiving a SAR during the school holidays

If you receive a SAR on the last day of the school term, or during the school holidays, you must still respond within one calendar month.

Education settings cannot extend a SAR response because it is the school holidays.

If you are unable to meet the legal deadline of one calendar month, you should let the requester know as soon as possible.

Charging for a SAR

You cannot charge a fee to complete a SAR. In some cases, you may be able to charge for administration costs associated with completing a SAR. For example, if the requester insists on having multiple copies of information, you could charge for the cost of printing. Read more about charging a fee on the ICO's website.

Information to include in a SAR response

Individuals have a right to know how their personal data is being used. A school's privacy policy will usually include this information. You should include a link to your school's privacy policy in your SAR response. The ICO has more details on what other information an individual is entitled to.

Education settings must make reasonable efforts to search through all records, including:

- emails (including those in deleted or trash folders)
- documents
- spreadsheets
- databases
- record systems
- CCTV
- USB sticks or CDs
- paper records in filing systems
- instant messages

Good data storage and retention policies make it easier to identify personal information.

Moving to a cloud-based system may help you prepare for subject access requests. Cloud-based systems also offer other security benefits. You can find out more information in the guidance on cloud solution standards for schools and colleges.

You can include extra or contextual information in a SAR response. You will need to explain that extra information is being provided outside of the requester's information rights.

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.

You should be able to evidence that the requester has already seen or had access to the information, in case you receive a complaint.

Redacting information

Depending on what the requester asks for, you may need to remove some information. This process is known as redacting. You should redact personal information that identifies anyone other than the person the SAR is about. This is known as removing third party information.

In some cases, you may need to release third party information. This decision must be made on a case-by-case basis, and you should record any decisions you make about releasing third party data.

Read more on information about other individuals on the ICO's website.

You may need to redact information about:

- other pupils
- other parents
- staff

When redacting identifiable information, make sure that redactions cannot be undone. You should use specific redaction software, such as Adobe Acrobat Pro.

Individuals may ask to see CCTV images of themselves or their child. CCTV images contain personal information. Images of other people appearing in CCTV images must be redacted, for example by blurring.

A SAR entitles a person to access their own personal information but does not entitle them to access full documents. You may extract personal information from a document to include in your SAR response, and provide context of where the information is held.

You should keep a copy of unredacted and redacted versions of information in case of review.

.

Information that is no longer available

In some cases, a requester may ask for information you no longer hold. You should respond by telling them the information is no longer held by you.

You can refer the requester to your data retention policy or privacy notice.

SAR response formats

Usually, a SAR response will be made in the same format as the request was received.

A written response is preferable, but if you receive a verbal request, you can provide a verbal response if the requester asks for one. You should make a written record of the response.

Make sure you submit the response in a secure way. You may want to submit the response by:

- encrypting the document
- saving the document in a secure workspace
- using tracked mail for physical documents

If delivering a response by hand, consider obtaining a signature to confirm receipt.

Making sure a SAR response is accessible

Education settings should make it simple for individuals who need additional support to make a SAR. You should make sure your response is in an accessible format that meets the needs of the requester.

Refusing to comply with a SAR

Schools can refuse to comply with a SAR if:

- a data protection exemption can be applied to all the personal information in scope of the request
- the request is manifestly unfounded or manifestly excessive

Examples of exemptions that may apply to education settings include:

- releasing the information would cause serious harm to a child
- releasing information would not be in the best interests of a child
- information relating to third parties
- legal advice sought and received from a lawyer
- information that may prejudice an investigation

Find out more about exemptions on the ICO website.

Manifestly unfounded SARs

A manifestly unfounded SAR is when an individual submits multiple SARs with malicious intentions.

For example, a parent submits a SAR every week with the intention of harassing a staff member following an earlier disagreement. The parent offers to withdraw their SAR for personal benefit.

Before refusing to comply with a request on these grounds it is important you can show the reasons why you think a request is not genuine.

A request might not be genuine if:

- it includes details of an intention to cause disruption
- it targets an employee with unproven accusations

Read more about manifestly unfounded requests on the ICO website.

Manifestly excessive SARs

A manifestly excessive SAR means that the effort and cost of collecting the information makes responding to the request unreasonable or disproportionate.

This is not an easy assessment to make. You will need to consider all the circumstances of the request before making a decision. The ICO provides comprehensive guidance about what factors need to be considered. Read more about manifestly excessive requests on the ICO website.

Notifying a requester about a refused SAR

You will need to notify a requester that their SAR has been refused within one calendar month from the day they made the SAR. You will also need to include the reason for the refusal. The requester should be given details about how to complain to the ICO or seek a judicial review.

Complaints about a SAR response

A SAR response letter must include the following information:

- organisation contact regarding the response, usually the data protection officer
- details on how to complain to the ICO
- acknowledgement of their right to seek judicial remedy
- acknowledgement of their other data protection rights such as the right to have their information deleted or changed

If the requester is unhappy with their SAR response, you should offer them the chance for their case to be reviewed. If the requester remains unhappy with the school's response, they can complain to the ICO. The ICO will consider the complaint and contact the school for further information or to provide advice as appropriate.

When an organisation processes a SAR, they should anticipate any future challenge or a formal ICO complaint. Completing a case review record while handling a SAR, which details what decisions you have made and why may serve as a useful tool when responding to complaints.

Recording the SAR process

Knowing where your school holds personal data will make it easier to find information when processing a SAR. You should keep a record of the SAR process from start to finish.

Recording the SAR process is especially helpful if a requester submits a complaint or if you are audited by the ICO.

You may want to record:

- the date the request was received
- any time the response was paused and why (for example getting identification)
- a copy of all correspondence
- information about which records and systems were searched and what was found
- any information that was redacted and the reason why
- the date you sent the response and a copy of it
- copies of any ongoing correspondence with the requester (such as confirmation of receipt, complaints)
- evidence of decision to refuse a SAR
- evidence of decision to exempt any information

Handling other information rights requests

How to manage other information rights requests, including changing, deleting or restricting the processing of personal information.

Information rights mean a person has the right to access or amend the personal data any organisation, such as a school, holds about them.

The most common type of information rights request is a subject access request (SAR). This is when someone requests to see the personal data an organisation holds about them. There is more information on to how to handle a SAR in a school.

Individuals, including children, have several information rights relating to personal data a school may hold about them.

Information rights request that someone might make include asking to:

- change inaccurate personal information you hold about them
- remove their personal information or record
- restrict the processing of their personal information
- stop processing their personal information (right to object)

You can receive an information rights request relating to personal data either verbally or in writing, including through social media.

Unless there's a valid reason, you must respond to any information rights request within one calendar month. If the case is complex you can extend the response deadline by an extra 2 calendar months.

Information rights requests only apply to the personal data you hold when you get the request.

Individuals have the right to request changes or restrictions to personal information, but a school is not obliged to make changes to data in certain circumstances.

Your school should have procedures in place for responding to information rights requests. You should also make sure that all staff are trained to recognise different kinds of information rights request and know how to escalate a request if they receive one.

Record keeping and management

How to carry out an audit to check what personal data your school holds. You can use a data retention schedule to document how long you'll keep different types of data for.

The Data Protection Act 2018 and UK GDPR says you should only keep data for as long as you need it. You should check each year what data you hold and if you still need to keep it.

If you identify any information you no longer need, you should dispose of it safely.

It's important to put in place policies and processes so you can prove and evidence that you're not keeping data for longer than necessary.

Develop a data retention policy

Your data retention policy should explain how long you need to keep information. It should set out:

- why you are holding this data
- your justification for keeping the data
- the lawful basis for processing and keeping the data
- if you will pass this data on and, if so, if you need to keep it once you have passed it on
- the steps you will take when you destroy any personal data

A good data retention policy includes how long you will keep data items within the different areas of school administration. For example, you may need to keep pupil names in your safeguarding system longer than in your catering system.

When setting a data retention policy, consider:

- why you are holding this data
- if there is a legal duty to keep the information for a set period of time
- whether you will need to share the data and, if so, whether you need to keep it after sharing it
- if it is more appropriate for another organisation such as the local authority to keep the information in the long term
- if you will need the data to meet Ofsted's requirements
- whether you can delete or depersonalise some of the information
- if you have a justification to keep the data

Carry out a personal data audit

You should carry out an audit of all the personal data you hold each year to check it is up to date and still needed. You must not keep any data longer than is necessary.

As part of your audit, include pupil and staff data in:

- paper records
- databases
- online systems
- videos and photos

Reviewing the personal data you hold will help you to identify what data you need to:

- keep
- destroy
- change from a paper format to an electronic format
- keep for research or litigation purposes

Consider grouping your data items about pupils into these areas:

- admissions
- attainment
- attendance
- behaviour
- exclusions
- personal identifiers, contacts and pupil characteristics
- identity management and authentication
- catering and free school meal management
- trips and activities
- medical information and administration
- safeguarding and special educational needs
-

Document the decision you make against each data item. Find out how to create a record of processing activity.

Share the results of your audit with your school leaders, governors and trustees. They are responsible for making sure the school is compliant with the Data Protection Act 2018 and only keeps the data it needs.

Depersonalise personal data

As data becomes older, there are steps you can take to keep data about pupils for analytical purposes. Before deleting the data completely, remove names and personal identifiers. For example, once the pupil has left your school, you could remove their name and date of birth. This will remove some of the risks around personal data. It will also allow you to use it for long-term analysis of trends.

Another option is to replace the personal information with non-personal identifiers. For example, you could replace the:

- name with a random ID
- date of birth with year of birth
- postcode with locality or town name

For some records, you may only need to keep summary statistics.

Dispose of personal data

When records have reached the end of their retention period, data must be disposed of securely and confidentially. The Information Commissioner's Office (ICO) has guidance on practical methods for destroying records that are no longer needed.

All records containing personal information or sensitive policy information must be made either unreadable or so you cannot reconstruct it.

Your data retention policy must include your procedures for safely destroying personal data. All staff should be aware of these procedures to help prevent any data breaches.

Do not dispose of records with the regular waste or in a skip.

You should:

- shred paper records using a cross-cutting shredder, or get an external company to shred them
- destroy storage media and hard disks to particles no larger than 6mm
- dismantle and shred audio and video tapes

If you use an external company to destroy records, it must:

- shred all records on-site in the presence of an employee
- be able to prove that the records have been destroyed and provide a certificate of destruction
- have trained its staff in the handling of confidential documents

The Freedom of Information Act 2000 requires you to maintain a list of records that have been destroyed and who authorised their destruction. You must have approval from a senior leader for the record to be destroyed.

You must document the destruction. Record a brief description of the data, the number of files and who authorised the destruction. Shred the records as soon as you've documented them as having been destroyed. Further guidance is available on record keeping and retention for academies and academy trusts.

Create a data retention schedule

Once you have your list of data item groups, consider creating a data retention schedule. This should state how long you'll hold certain types of personal data before destroying it.

How long you keep different types of data will depend on whether you're keeping it for operational needs or to comply with legal requirements.

The following records have statutory retention periods.

You should decide how long you need to keep other records, in line with the business need of your school.

Refer to the school Retention of Documents Policy 2026

Managing breaches of data

Good practice for preventing personal data breaches in your school. It explains how to recognise and respond effectively to a personal data breach.

A data breach is a security incident that has resulted in personal data you hold being:

- lost or stolen
- destroyed without consent
- changed without consent
- accessed by someone without permission

Data breaches can be deliberate or accidental. A breach is about more than just losing personal data.

Identify and investigate a personal data breach

UK GDPR places certain legal obligations onto organisations relating to the handling of personal data breaches. It is important to make sure that you're properly prepared to handle such a breach.

You can find more guidance on personal data breaches on the Information Commissioner's Office website.

Identify a personal data breach or a suspected personal data breach

The first step is to make sure that all members of staff:

- are able to recognise when a personal data breach has taken place
- know how to report it formally within your school

Your school's data protection officer should:

- support you throughout the process
- where necessary, liaise with the Information Commissioner's Office

Check if any personal data is involved

Once you become aware of a suspected personal data breach, you need to check if the incident involves personal data. If it does, there are actions you'll need to take.

Understand the type of personal data involved

This is an important step in understanding the seriousness of the breach. You'll need to understand as soon as possible:

- what types of personal data are involved
- who the data subjects are

For example, is it:

- basic personal details of staff, such as name and email addresses
- full records of pupils, including special category data such as disabilities and ethnic origin

Take action to limit further impact

Your priority is to establish what has happened to the personal data. You need to find out where the personal data that has been accessed, lost or stolen now is, and who might have it. This will affect the level of risk involved. For example, if you've shared some information via email by mistake with another part of your school or trust, this is much less of a risk than an unknown party stealing paper records. If you can recover the data, you should do so immediately. You should do whatever you can to protect those who'll be most impacted.

This might include:

- recalling, or asking someone to delete, an email containing personal data sent by mistake
- retracing your steps or contacting reception if you have physically lost some personal data to see if it has been handed in
- checking if you can lock or wipe a laptop, phone or tablet containing personal data that has been stolen remotely

Work out how many data subjects might be affected by the breach

You need to be aware of how many people are affected by the breach. This will help you determine the level of risk involved.

Assess the severity of the personal data breach

It is important to make sure that you accurately record all details of the breach. You may need to make an assessment before you have the full details. Based on the information you have so far, you should assess the risk to the data subjects involved.

Risk, in terms of a personal data breach, means the risk to the people who are affected. You're assessing how seriously you think people might be harmed and the probability of this happening.

Consider all the information currently available, for example:

- who's affected
- how many people are affected
- the ways it might affect them, such as:
    - safeguarding issues
    - identity theft
    - significant distress

When assessing risk, put yourself into the shoes of those who've been impacted. This may help you think about any steps you can take to reduce that risk.

If you're unsure, get help and support from the Information Commissioner's Office.

Report the personal data breach

If you decide that there is a risk to data subjects:

- notify the Information Commissioner's Office within 72 hours of becoming aware of it
- inform data subjects, so they can take steps to protect themselves

If you're unsure how best to handle a breach, call the ICO helpline on 0303 123 1113. They'll support you assess the impact and appropriate steps, including how to let data subjects know.

Report a personal data breach to the Information Commissioner's Office.

Review the personal data breach

After every personal data breach or near miss, you should review:

- what happened
- how it happened
- why it happened
- what actions you can take to prevent it happening again

Do this even if you have determined there are no risks.

It is good practice to record and investigate every personal data breach, however small. Recording every incident allows your data protection officer to spot any trends. If they notice that a particular system or process is regularly having minor incidents, they can reduce the risk and take action to prevent similar breaches from happening again. You should always make sure you document all lessons and actions you've taken.

How to prevent a personal data breach

It is important to take steps to reduce the possibility of personal data breaches occurring. This might include:

- having mandatory data protection training in place for all staff that includes how to recognise and report a personal data breach
- having clear and appropriate data protection policies
- ensuring staff have an awareness of common data breaches and how they can be avoided, such as by checking recipients and attachments are correct before sending emails
- having appropriate controls in place to protect personal data

Generative artificial intelligence (AI) and data protection in schools

How to address potential data protection risks of using generative AI in schools.

Generative AI refers to any type of artificial intelligence that creates new digital content, such as text, images, videos or other data. Unlike traditional AI, which relies on exact programming to complete specific tasks, generative AI uses machine learning to create new digital content.

This guidance is to help schools understand:

- how to protect personal data when using generative AI
- data protection legislation in relation to generative AI
- the risks and biases of AI to personal data

Watch the Department for Education (DfE) training video 'Protecting children's privacy when using artificial intelligence'.

In a school, generative AI tools can be used as a starting point to develop resources, including:

- lesson plans or activities
- questions and quizzes
- revision activities
- images to help with character descriptions or stories
- communications for parents and carers
- creating timetables

Check with your data protection officer or IT lead for further guidance on what may be acceptable use for your school.

Data protection and AI tools in education

Generative AI tools could offer significant benefits in education, but they come with certain risks related to data protection.

Schools should be open and transparent about how they use generative AI tools. Staff, students, governors, parents and carers should understand how their personal data is processed.

Ofsted has published guidance on the ways it expects providers to use AI.

The Joint Council for Qualifications (JCQ) guidance on AI use in assessments sets out best practice for students and teachers, to help them understand their responsibilities where AI tools are being used as part of qualification assessments.

Open and closed generative AI There are important differences between open and closed generative AI tools in terms of data protection.

Open generative AI tools are accessible and modifiable by anyone. They may store, share or learn from the information entered into them, including personal or sensitive information. You should avoid including any identifiable information in the data you enter into open AI tools, to protect personal and special category data.

Closed generative AI tools are generally more secure, as external parties cannot access the data you input. This makes them a safer option for handling personal or special category data.

It's not always obvious whether a generative AI tool is open or closed. Check with your school's data protection officer or IT lead to find out more about the generative AI tools available at your school.

If your school has a closed generative AI tool and you choose to put personal or special category data into it, you must include how you use this data in your school's privacy notice.

Compliance with data protection legislation

The generative AI tools you use must comply with data protection legislation and your school's data protection notice.

To protect data when using generative AI tools, you should:

- seek advice from your data protection officer or IT lead
- check whether you are using an open or closed generative AI tool
- ensure there is no identifiable information included in what you put into open generative AI tools
- acknowledge or reference the use of generative AI in your work
- fact-check results to make sure the information is accurate

Personal data collected by generative AI tools

Some generative AI tools process and store more information than just the text you enter into them. Generative AI tools may collect and store additional data such as:

- location
- IP address
- system information
- browser information

The data collected by these organisations can be viewed or sold to third parties. Schools must include how any data is collected, processed and stored by generative AI tools in the school's privacy notice.

Download resources to help with data protection in schools, including posters, templates, and learning materials.

Artificial intelligence

Do you need to use AI? Need, Read, Proceed (PDF, 205 KB)

Do you need to use AI? Need, Read, Proceed - low ink version (PDF, 186 KB)

Protect children's privacy when using AI (PDF, 168 KB)

Protect children's privacy when using AI - low ink version (PDF, 152 KB)

Checklist to protect children's privacy when using AI (PDF, 187 KB)

Checklist to protect children's privacy when using AI - low ink version (PDF, 169 KB)

Protecting children's privacy when using Artificial Intelligence

https://youtu.be/Hs6gmNoMhqM

Resources to support data protection in schools

Data protection in schools - Resources to support data protection in schools - Guidance - GOV.UK