Thurgoland CE Primary

UK GDPR Data Protection Policy

Approved by: Full Governing Body
Date Approved: 08.07.2026
Review Date: July 2027
Policy Owner: Full Governing Body

Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with relevant legislation.

With recent changes to the UK's relationship with the European Union, the policy reflects the new UK GDPR (General Data Protection Regulation) and the Data Protection Act (2018)

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Legislation and guidance

This policy meets the requirements of the UK GDPR and DPA 2018. The policy reflects guidance issued by the Information Commissioner's Office (ICO) and Information and Records Management Society.

Please note that from April 2026, the ICO will be known as the Information Commissioner.

In addition, the policy sets out good practice issued by the National Cyber Security Centre on the security of electronic data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

The policy covers the following legislation
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA)
- School Standards and Framework Act 1998
- Freedom of Information Act 2000
- Electronic Commerce (EC Directive) Regulations 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- Protection of Freedoms Act 2012
- Data Access & Use Act 2025 (DUAA)
- Employment Rights Act (1996)

This policy also has regard to the following guidance:

- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO (2012) 'IT asset disposal for organisations'
- DfE (2018) 'Data protection: a toolkit for schools'
- DfE (2026) 'Keeping Children Safe In Education''

- Information Sharing Advice for Safeguarding Practitioners (DfE)
- Information Sharing Duty: Statutory Guidance (September 2026)

This policy will be reviewed and updated in phases as the DUAA provisions come into force. We will monitor ICO guidance and adjust accordingly.

Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: ● Name (including initials) ● Identification number (or Unique Pupil Number) ● Location data ● Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: ● Racial or ethnic origin ● Political opinions ● Religious or philosophical beliefs
	● Trade union membership ● Genetics ● Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes ● Health – physical or mental ● Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

The governing body is the data controller. The headteacher is responsible for operational oversight of data protection compliance.

The Information Asset Owners (IAO) for the school is the headteacher and governing body.

Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action. In addition, any member of staff who reports another member of staff violating the data protection principles is protected by the school's Whistleblowing Policy.

Governing body

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations. It is recommended that a member of the governing body is given the role to oversee data protection compliance. Data protection should be an agenda item at every full governors meeting, so the school's compliance can be reviewed.

Data protection officer
The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.
They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Mr Tim Pinto from The E-Safety Office Ltd and is contactable via the School Office.

Headteacher
The headteacher acts as the representative of the data controller on a day-to-day basis. Some of the tasks related to this may be delegated to other members of staff.

All staff
Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data to a 'third country'
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

Data protection principles

The UK GDPR is based on data protection principles that our school must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner

- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure.

This policy sets out how the school aims to comply with these principles.

Collecting personal data

Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect or safeguard someone's life, safety or wellbeing
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018.

The school uses a number of online services to support the teaching and learning and safeguarding of children in the school. This falls under the legitimate interests of processing, however some services do need explicit consent and we contact parents directly.

We may use some services where the parent has to register their details with a third party company e.g. catering services. On these occasions, the school will highlight the privacy notice of the third party company.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

In addition to existing lawful bases (such as consent, legitimate interests), we may make use of the new lawful basis of recognized legitimate interests (Article 6(1)(ea)) for certain processing (e.g., safeguarding, security, emergency response). Where this is adopted, we will document the rationale and apply appropriate safeguards.

Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This must be done via a secure manner using a cross shredder or secure bin. Any destruction of a large amount of data must be logged by the data protection lead in school.

Paper data that has to be retained for a specific period of time, must be kept in an archived area which has restricted access. Only specific staff are allowed access to this area.

In addition, staff should follow the retention schedule for electronic data and must ensure that they use a file system to ensure that data can be easily accessed.

This will be done in accordance with the Information and Records Management Society's toolkit for schools.

We maintain up-to-date records of processing activities, DPIAs, risk assessments, and algorithmic governance documentation, incorporating the changes introduced by the Data (Use and Access) Act.

Sharing personal data
We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this, unless the law and our policies allow us to do so, in accordance with Keeping Children Safe in Education Statutory Guidance, Information Sharing Advice for Safeguarding Practitioners (DfE) and the Information Sharing Duty: Statutory Guidance (September 2026).

- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law

    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share

    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings

- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

As the UK is now classed as a 'third country' it will ensure that it obtains a Standard Contractual Contract with data processed outside the European Economic Area.
When transferring personal data outside the UK, we will ensure that protections equivalent to or not materially lower than UK standards apply, using safeguards such as standard contractual clauses, binding corporate rules, or other mechanisms.

Subject access requests and other rights of individuals

Subject access requests
Dealing With Subject Access Requests
Introduction
In 2018, the DfE produced a toolkit for schools on data protection. This has recently been updated and includes revised information on dealing with s 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.
Individuals can make a SAR in any format. It could be:
Verbal request
Written – via letter, text or email.
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

Clarifying a SAR
Some requests will be non-specific and ask for "all the information you hold".
You cannot ask the requester to narrow or reduce their request. You can ask for clarification of what specific information the requester is looking for. This might be helpful when the requester asks for a lot of information because they are not sure what they need.

When to check the identity of someone submitting a SAR
In most cases when an individual makes a SAR you will need to ask for identification (ID) from them.
In a school setting, pupils and their parents or carers are generally well-known to school staff. If you know the requester and are sure of their identity and authority, you do not have to request ID. Make a record of why you made this decision.

If the requester is asking for their own information, and you do not know them, then they will need to provide their identification.

Adults should provide a photo ID plus another form of ID, this could be:
- their driving license or passport for the photo ID
- a utility bill or council tax bill that confirms their name and address.

If the requester is asking for another individual's information, then they will need to provide the individual's ID.
They will also need to provide evidence that they have the authority to act on the individual's behalf. This includes requesters such as parents and solicitors.

Responding To A Request From A Child
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.

Under 13 - 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.

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.
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.
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.

Example
A parent collects their 8-year-old from school. Whilst waiting for their child, the parent tells a teaching assistant that they wish to see copies of their child's personal information relating to the school's handling of an incident that recently occurred on school premises involving their child. Usually, the school encourages parents to make a SAR by emailing the request to office@thurgolandprimary.org. The teaching assistant asks the parent if they can complete the request via email. The parent insists they want to make the request verbally.

The teaching assistant writes down contact details for the parent, details of the child and an overview of the verbal request. The teaching assistant checks that the parent is happy for future correspondence to be made in writing and immediately passes the request to the Data Protection Officer. The Data Protection Officer knows the parent and child well and decides not to request ID. The Data Protection Officer sends the parent a letter to acknowledge the SAR and to clarify the request.

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.
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.

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.

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.

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.

Information to include in a SAR response

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

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.

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.

Example

Ebony Smith's dad has submitted a SAR requesting Ebony's behavioural record.

The school office's record reads:

'Ebony Smith was excluded due to a fight she had with Sajid Khan'. When the school responds to the SAR, it should read 'Ebony Smith was excluded due to a fight she had with (REDACTED)'.

Although Ebony's dad might know who the fight was with, the school should not release this information. Ebony's dad is only entitled to the personal data held about Ebony, not Sajid.

Example

A child has submitted a SAR for all information the school holds about their special educational needs.

The school identifies the child's personal information is contained in the minutes of a governors' meeting.

The child's personal information in scope of the request amounts to 2 sentences within a 4-page document. The rest of the document is not about the child.

The school extracts the child's personal information for inclusion in their response. They do not provide the whole document.

The school provides the requester with context about where the information is held. The remaining information is out of scope of the SAR and is not released.

SAR Response Format

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.

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.

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.

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.

Example

A school receives a SAR from the absent parent of a child aged 16. The requester has asked for details of the college they now attend.

This request immediately raises a red flag, that releasing the information may not be in the best interest of the child. Also, if the requester had a relationship with their child, it would be reasonable to expect that they would already know this information.

The school acknowledges the SAR and asks the requester to provide:

- identification and proof of their link to the child, such as a birth certificate
- any parental agreement or court order that may be in place

This is to establish parental responsibility and any restrictions to the requester's parental role.

The parent provides their own identification and a copy of the child's birth certificate and states no agreement or court order is in place. This means the school now has the requester ID and parental responsibility status.

The school contacts the child for consent to release the information, as they are aged 13 or over. The school also checks information and records they hold about the child.

The child asks the school not to release any of their personal information to the requester. The child states they have no relationship with their absent parent, due to historic emotional abuse towards them and their resident parent. The child feels releasing the requested information would adversely affect their mental health.

The school considers the rights of the parent and those of the child. As there is a risk to the child's wellbeing, they make the decision not to release the child's information.

In this case the child's data protection rights exceed parental rights, and the SAR is refused.

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.

Individuals wishing to make a complaint about how we handle their personal data should submit it to Mr Dale Jordan. We will acknowledge the complaint within 30 calendar days and respond without undue delay. If the complainant remains dissatisfied, they may escalate the matter to the Information Commissioner's Office.

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.
- 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.

If staff receive a subject access request they must immediately forward it to the headteacher.

9.2 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest

- Request a copy of agreements under which their personal data is transferred to a third country
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine- readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO (through the school office). If staff receive such a request, they must immediately forward it to the DPO.

Parental requests to see the educational record

Parents, or those with parental responsibility, may have access to their child's educational record (which includes most information about a pupil that the school holds on their MIS system) within 15 school days of receipt of a written request.

Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.
We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:
- Within school on notice boards and in school brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website
- Educational Apps *
- Social media pages *
- Video sharing platforms *

* Please note that these are third party platforms and if images are shared, parents should be directed to their specific private policies.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the specific photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with their names. See our E-Safety Policy for more information on our use of photographs and videos.

Data protection by design and default
We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law.
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

Data security

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
In particular:

- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Strong passwords, in line with the school's cyber security requirements, are used to access school computers, laptops and other electronic devices. Staff are required to change their passwords at regular intervals
- Staff remote access to the school's network from a school's device is via an encrypted private network (VPN)
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected
- Please see the Information Security Policy for further details

Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in the Data Breach Policy. When appropriate, we will report the data breach to the ICO within 72 hours.

Artificial Intelligence

The School recognises that Artificial Intelligence (AI) tools may be used to support administrative, educational and operational activities. Any use of AI involving personal data will be lawful, transparent and proportionate, and will comply with the UK General Data Protection Regulation, the Data Protection Act 2018 and the Data Access & Use Act 2025. Staff, governors and volunteers must not input personal data, special category data or confidential information about pupils, parents, staff or the School into AI systems unless the tool has been formally approved, appropriate contractual safeguards are in place, and a Data Protection Impact Assessment (DPIA) has been completed where required.

AI must not be used for automated decision-making about pupils or staff where such decisions produce legal or similarly significant effects, unless explicitly permitted by law and subject to appropriate human oversight. The School will ensure that AI use supports safeguarding, data minimisation and security principles, and that all users receive appropriate guidance and training on the responsible and ethical use of AI.

Training

All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every year** and shared with the full governing board.

Links with other policies/documents

This data protection policy is linked to our:

- Safeguarding Policy
- Data Breach Policy
- Online Safety Policy
- Bring Your Own Device Agreement
- Artificial Intelligence Policy
- Acceptable Use Agreement
- Cyber Response Plan