Nurturing to Learn

GDPR AND DATA PROTECTION POLICY

Governing Body Ratification Date: April 2026
Issue Date: April 2026
Next Review Date: April 27
Responsible Person(s): John Dexter

UK GDPR and Data Protection Policy

This policy should be read alongside the school's privacy notices, retention schedule, records of processing, breach response procedure, acceptable use / information security procedures, and data sharing arrangements.

1. Purpose and scope

This policy sets out how the School will comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), and related guidance that applies to schools.

It applies to all personal data processed by or on behalf of the School, whether held electronically, on paper, in images, audio, CCTV, or in any other format.

It applies to governors, leaders, staff, agency workers, volunteers, contractors and any other person who processes personal data for the School.

The School is committed not only to complying with the law, but also to being able to demonstrate that it complies through clear governance, records, staff training and effective day-to-day practice.

2. Policy objectives

The School will process personal data lawfully, fairly and transparently.

The School will protect the rights and freedoms of pupils, parents, carers, staff, governors, volunteers and other individuals whose data it processes.

The School will ensure that staff understand their data protection responsibilities and know how to recognise and escalate risks, incidents and requests.

The School will maintain appropriate policies, procedures, records and safeguards so that compliance can be evidenced and reviewed.

3. Roles and responsibilities

The School is the data controller for the personal data it processes for its own purposes.

The governing body and senior leaders are responsible for oversight of data protection compliance, risk and resourcing.

A Data Protection Officer (DPO) is appointed to advise the School, monitor compliance, support data protection impact assessments, and act as a point of contact with the Information Commissioner's Office (ICO).

All staff are responsible for handling personal data securely, following School procedures, completing required training, and reporting concerns or breaches immediately.

Where the School uses processors or third-party services, it will carry out appropriate due diligence and ensure that written contracts contain the requirements of Article 28 UK GDPR.

4. The data protection principles

The School will comply with the seven principles in Article 5 UK GDPR. Personal data must be:

- processed lawfully, fairly and in a transparent manner
- collected for specified, explicit and legitimate purposes and not further processed incompatibly
- adequate, relevant and limited to what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- processed securely using appropriate technical and organisational measures
- processed in a way that allows the School to demonstrate accountability.

5. Lawful basis for processing

The School will identify and record an appropriate lawful basis under Article 6 UK GDPR before processing personal data.

In most school contexts, processing is likely to rely on one or more of the following: legal obligation, public task, contract, vital interests, legitimate interests (where applicable), or consent where this is genuinely appropriate.

Consent will not be used where the School cannot offer a real choice or where another more appropriate lawful basis applies.

Privacy notices and records of processing will explain the lawful basis or bases relied on for each main processing activity.

6. Special category and criminal offence data

Where the School processes special category data, it will identify both an Article 6 lawful basis and an Article 9 condition. Where relevant, it will also identify the Schedule 1 condition required by the DPA 2018.

Where criminal offence data is processed, the School will ensure that an appropriate legal basis and DPA 2018 condition is identified and documented.

The School will only process this information where it is necessary, proportionate and supported by suitable safeguards, including access controls, confidentiality and retention arrangements.

7. Accountability, documentation and record keeping

The School will maintain and keep under review records of processing activities, privacy notices, retention arrangements, breach logs, data sharing records, consent records where consent is used, DPIA records, and processor contracts.

The School will conduct periodic information audits to understand what personal data it holds, where it came from, who it is shared with, how long it is kept, and what risks attach to it.

Leaders will review data protection compliance regularly and take action where audits, complaints, incidents or practice identify gaps.

8. Privacy notices and transparency

The School will provide privacy information in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Separate privacy notices will normally be maintained for pupils and parents, workforce, governors/volunteers, and any other group where tailored transparency information is needed.

Privacy notices will explain, as applicable, what information is collected, why it is processed, the lawful basis, who it is shared with, whether data is transferred internationally, how long it is kept, and how rights can be exercised.

Where the School shares data with the Department for Education or other bodies, privacy notices will explain this clearly.

9. Data minimisation, accuracy and retention

Staff must only collect, use and share the personal data that is necessary for the relevant purpose.

Personal data must be accurate and, where necessary, updated without undue delay.

The School will maintain a retention schedule and dispose of records securely when they are no longer required.

Retention decisions must reflect statutory requirements, business need, safeguarding considerations and accountability obligations.

10. Individual rights

Individuals have rights under UK GDPR, including the rights to be informed, access personal data, rectify inaccurate data, erase data in certain circumstances, restrict processing, object, and - where applicable - data portability.

Individuals also have rights in relation to complaints, breaches presenting high risk, and solely automated decision-making with legal or similarly significant effects.

The School will have arrangements in place to recognise, log, assess and respond to information rights requests within the applicable timescales.

11. Subject access requests and education records

A subject access request (SAR) can be made verbally or in writing and does not need to mention the UK GDPR to be valid.

The School will verify identity where reasonable and proportionate before disclosing personal data.

The usual time limit for responding to a SAR is one calendar month from receipt of the request or, where permitted, from receipt of any information reasonably needed to confirm identity or clarify the scope of the request.

The School may extend the response period by up to a further two months where requests are complex or numerous. If so, the requester will be informed within the initial one-month period and told why.

Parents of pupils at maintained schools have a separate right to inspect their child's educational record free of charge within 15 school days under the Education (Pupil Information) (England) Regulations 2005.

When considering requests involving children, the School will consider the child's competence, understanding, rights, and best interests rather than relying on a fixed age threshold.

Where a person with parental responsibility makes a request on behalf of a child, the School will assess whether the child is able to exercise the right themselves and whether disclosure to the parent is appropriate in the circumstances.

The School may withhold or redact information where an exemption applies, including where disclosure would adversely affect the rights and freedoms of others or where another relevant exemption under data protection law or education law applies.

12. Automated decision-making, profiling and AI-enabled tools

The School does not expect to make solely automated decisions that have legal or similarly significant effects on individuals unless this is lawful, necessary and appropriately safeguarded.

If the School uses profiling, analytics or AI-enabled tools, leaders will assess the privacy and safeguarding implications, determine whether a DPIA is required, and ensure that any use is transparent, proportionate and properly governed.

Solely automated decision-making with legal or similarly significant effects will only be used where authorised by law, necessary for a contract, or based on explicit consent, and the individual will be given the safeguards required by Article 22 UK GDPR.

13. Data protection impact assessments (DPIAs)

The School will apply data protection by design and by default.

A DPIA will be completed where processing is likely to result in a high risk to the rights and freedoms of individuals, for example when introducing new technologies, large-scale monitoring, or new categories of high-risk processing.

DPIAs will consider necessity, proportionality, risks, mitigation, residual risk and whether consultation with the DPO or ICO is required.

DPIAs will be kept under review where processing changes.

14. Information sharing and safeguarding

Personal data will only be shared where there is a clear legal basis, a valid purpose, and appropriate safeguards.

The DPA 2018 and UK GDPR do not prevent appropriate information sharing for safeguarding purposes. Staff must follow safeguarding procedures and seek advice where needed, but must not allow uncertainty about data protection law to delay the sharing of information where a child is at risk.

The School will keep appropriate records of routine and non-routine sharing where this is required for accountability.

15. Processors and third-party services

Where personal data is processed on the School's behalf, the School will ensure that processors provide sufficient guarantees about security, confidentiality, compliance and support for data subject rights.

Contracts with processors will set out the subject matter, duration, nature and purpose of the processing, the types of data, categories of data subjects, and the processor's obligations.

The School will carry out proportionate due diligence before using new systems or providers, including checking hosting arrangements, security standards, retention, international transfers and subcontracting.

16. International transfers

The School will identify whether any personal data is subject to a restricted transfer from the UK.

Where a restricted transfer is made, the School will ensure that the transfer is covered by UK adequacy regulations or by another lawful transfer mechanism and risk assessment recognised under UK GDPR and ICO guidance, such as the International Data Transfer Agreement (IDTA) or the UK Addendum where appropriate.

The School will record relevant transfer decisions and safeguards in its contracts, privacy information and records of processing where applicable.

17. Information security

The School will use appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

These measures will include, where appropriate, role-based access controls, secure passwords and authentication, encryption, secure disposal, backup arrangements, device controls, appropriate use of email, and physical security.

Staff must follow the School's information security, acceptable use, remote working and records management procedures.

Personal data must not be stored on personal devices or local drives unless this is explicitly authorised and appropriately secured.

18. Personal data breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

All actual or suspected personal data breaches must be reported immediately in line with the School's breach procedure.

The School will assess each incident promptly, take steps to contain and recover the situation, record the facts, effects and remedial action, and decide whether notification to the ICO and affected individuals is required.

Where the breach is notifiable to the ICO, this will normally be done without undue delay and, where feasible, within 72 hours of becoming aware of it.

19. Training, monitoring and compliance

The School will provide induction and refresher training appropriate to staff roles.

Leaders will monitor compliance through audit, review of incidents and requests, spot checks where appropriate, and review of policies and procedures.

Failure to comply with this policy may lead to disciplinary action and, where appropriate, contractual action or referral.

20. Review

This policy will be reviewed at least annually and earlier where guidance, technology, organisational arrangements or legal requirements change.

The School will also review related procedures and notices to ensure they remain aligned in practice.

Appendix 1 - operational expectations for subject access and information rights requests

Staff must recognise and escalate any request about personal data, deletion, correction, restriction, objection or access, even where it is made informally or verbally.

The School should keep an information rights log showing the date received, requester, type of request, identity checks, clarification sought, deadline, outcome and any exemptions applied.

Where information includes third-party data, safeguarding information or confidential references, advice should be taken before disclosure.

Responses should be clear and secure, and the School should keep a record of what was disclosed and why.

Appendix 2 - local contacts and linked documents

Insert the School's named DPO, SAR contact point, breach reporting route, retention schedule reference, privacy notice links and related procedures before approval.

Appendix 3 - school-specific operational areas

Biometric recognition systems

If the School uses any biometric recognition system, such as cashless catering, library access or door entry, it will comply with the Protection of Freedoms Act 2012 as well as the UK GDPR and the DPA 2018.

Before using pupils' biometric information, the School will provide clear written information to parents and pupils, obtain the written consent required by law from each parent with parental responsibility unless an exemption applies, and respect any objection made by the pupil or by a parent.

Where biometric systems are used for staff, the School will ensure that use is lawful, necessary, proportionate and supported by an appropriate lawful basis, privacy information, retention controls and security measures. Alternative methods of access will be available where required.

CCTV and surveillance systems

Where CCTV or other surveillance systems are used, the School will ensure that they are deployed for a clear and legitimate purpose such as site security, safeguarding, the prevention and detection of crime, or the protection of pupils, staff and property.

The School will assess necessity and proportionality, maintain appropriate signage and privacy information, restrict access to footage, apply retention periods, and ensure that footage is only disclosed where there is a lawful basis to do so.

Any significant new surveillance use, or any use that is likely to create a high risk to individuals' rights and freedoms, will be considered through a DPIA before implementation.

Photographs and videos

Photographs, video recordings and similar images that identify individuals are personal data where the individual can be recognised. The School will process images lawfully, fairly and transparently and will make clear the purpose for which they are taken and used.

The School will follow its agreed permissions process for promotional or publicity use, will apply additional care where images are used online or shared more widely, and will ensure that safeguarding considerations are taken into account before any publication.

Staff must use school-approved devices, platforms and storage arrangements for school images unless expressly authorised otherwise. Personal devices must not be used in ways that conflict with safeguarding, data protection or records management requirements.

Monitoring arrangements

The governing body and senior leaders will receive periodic assurance about data protection compliance through policy review, audit activity, review of incidents and near misses, information rights logs, DPIA activity, training completion, processor due diligence and follow-up of any actions required.

The DPO will support monitoring activity by advising leaders, reviewing practice, identifying areas of risk and reporting themes or concerns so that compliance can be strengthened over time.

Links with other policies and procedures

This policy should be read alongside the School's privacy notices, retention schedule, breach procedure, records management arrangements, acceptable use and online safety arrangements, safeguarding and child protection policy, CCTV policy where used, biometric policy where used, remote working guidance, and any relevant use of AI or digital systems guidance.

Where a linked policy or procedure sets out more detailed operational steps, staff must follow that document alongside this policy.

Appendix 4 - personal data breach procedure

This appendix expands section 18 and should be used as the School's operational response when a personal data breach or suspected breach is identified.

1. Any member of staff, governor, volunteer, contractor or processor who discovers or suspects a personal data breach must report it immediately using the School's agreed reporting route. Delay can increase risk and may affect the School's ability to meet legal deadlines.

2. The DPO or nominated lead will assess whether a breach has occurred, contain and recover the situation where possible, and record the facts, categories of data involved, individuals affected, likely consequences and mitigation steps taken.

3. The School will decide whether the breach must be notified to the ICO and whether affected individuals must also be informed. Notifiable breaches will normally be reported to the ICO without undue delay and, where feasible, within 72 hours of the School becoming aware of them.

4. Where individuals must be informed, the School will communicate in clear language what happened, the likely consequences, the actions already taken, and any practical steps the individual should take.

5. The School will keep a breach log recording all breaches and near misses, decisions made, rationale for notification or non-notification, remedial action, and lessons learned. Leaders will review themes so that systems and training can be improved.

6. Breach response must be coordinated with safeguarding, HR, disciplinary, IT security and communications processes where relevant so that the School's response is lawful, proportionate and well evidenced.