OneEducation
Putting children first

# Data Protection Policy and Procedure

September 2025

This model policy and procedure has been produced by One Education's HR and People service. The HR and People team provides management and HR support and advice to schools and academies purchasing their services under an agreed Service Agreement. For further information please contact the HR and People team via the Helpline: 0161 276 0153 or Email: hrpeople@oneeducation.co.uk Website: www.oneeducation.co.uk

This policy is recommended for adoption by all maintained schools including community, voluntary controlled, community special, maintained nursery, foundation, foundation special and voluntary aided schools. It is also recommended for adoption by academies and free schools (modified as appropriate and taking into account the particular circumstances of the relevant academy or free school). Some school or academy specific provisions are included. This policy should therefore be adapted as necessary and inappropriate provisions deleted. The HR and People team can assist in adapting this policy to fully reflect a school's status including their academy or multi academy trust (MAT) status.

References in this policy to schools include a reference to academies and free schools unless otherwise stated. References in this policy to the Headteacher include a reference to an academy or free school Principal and references to the governing body include references to governing boards and/or trust boards as applicable.

| **Document Control** | |
|---|---|
| Title | **Data Protection Policy and Procedure** |
| Date | **September 2025** |
| Supersedes | N/A |
| Amendments | Updated in relation to the Data (Use and Access) Act 2025 ("DUAA") and to also include guidance on the use of artificial intelligence. |
| Related policies/guidance | **Freedom of Information Policy and Procedure, Artificial Intelligence policy** |
| Review | 2 years |
| Author | HR and People, One Education Ltd |
| Date consultation completed | |
| Date adopted by Governing Body | March 2026 |

**Equality Statement**: - Under the public sector equality duty (PSED), all schools/academies must have due regard to the need to eliminate discrimination, harassment and victimisation and any other conduct prohibited by the Equality Act 2010; to advance equality of opportunity between those who share a relevant protected characteristic and those who do not share it and to foster good relations across all protected characteristics. This means schools/academies must take into account equality considerations when policies are being developed, adopted and implemented.

The One Education HR and People team regularly reviews all policies and procedures which are recommended to schools/academies to ensure compliance with education and employment legislation including the Equality Act 2010. Consultation with schools/academies is an important part of this review process. Headteachers, Principals and Governing Bodies are asked to contact the HR and People team via the Helpline if they believe there are any negative equality impacts in their school/academy in relation to the application of this policy/procedure.

# Contents

## 1. INTRODUCTION

1.1 The school collects a large amount of personal data about staff, pupils, parents, governors, visitors and other individuals. The school aims to ensure that all such personal data is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 and guidance published by the Information Commissioners Office (ICO).

1.2 Personal information is any information that relates to a living individual who can be identified from the information regardless of whether it is in paper or electronic format.

1.3 This policy explains the duties and responsibilities placed on the school under the legislation relating to data protection to ensure that all data is handled and stored securely.

## 2. THE DATA (USE AND ACCESS) ACT 2025

2.1 The school is committed to keeping its data protection practices aligned with current legislation. In addition to complying with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Privacy and Electronic Communications Regulations (PECR), this policy reflects key developments introduced by the **Data (Use and Access) Act 2025** ("DUAA").

2.2 The DUAA, which received Royal Assent on 19 June 2025, introduces amendments to existing data protection laws. It aims to simplify compliance, support responsible innovation, and maintain high standards of privacy and data security.

2.3 Relevant changes for schools include:

- **Subject Access Requests (SARs):** The Act introduces a 'stop the clock' mechanism. This allows the school to pause the SAR response time where clarification is required from the requester, helping ensure proportionate and manageable handling of complex requests.
- **Automated Decision-Making:** A more permissive framework is introduced for decisions made solely through automated means. Where used, the school will ensure individuals are provided with meaningful information, the right to challenge decisions, and access to human review.
- **Children's Data Protection:** The Act strengthens obligations for online services likely to be accessed by children. The school will ensure that educational platforms and digital tools used comply with enhanced safeguards aligned with the Age Appropriate Design Code.
- **Recognised Legitimate Interests:** A new lawful basis for processing personal data has been introduced for specific activities such as safeguarding, preventing crime, and responding to emergencies. Where applicable, the school may rely on this basis without a full legitimate interests' assessment, as permitted by the DUAA.
- **Cookies and Similar Technologies:** The Act provides exemptions from the need for consent for certain low-risk uses of cookies and similar storage/access technologies, simplifying the use of tools like web analytics or accessibility features on the school website.

2.4 These changes will come into effect gradually over a 2–12-month period following Royal Assent. The school will review this policy and its practices as commencement regulations and official guidance from the Information Commissioner's Office (ICO) are published.

## 3. SCOPE

3.1 This policy relates to all employees, volunteers, contractors, pupils and parents. It also explains how members of the public may request information held by the school.

## 4. THE DATA CONTROLLER

4.1 The school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

## 5. DATA PROTECTION PRINCIPLES

5.1 The 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.

## 6. ROLES AND RESPONSIBILITIES

6.1 The Governing Board.

- The governing board has overall responsibility for ensuring that the school complies with all relevant data protection obligations.

6.2 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 i**s Judicium Education** and is contactable via dataservices@judicium.com and 0345 548 7000.

-

6.3 Headteacher.

- The headteacher acts as the representative of the data controller on a day-to-day basis.

6.4 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 outside the European Economic Area
  - 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

## 7. COLLECTING PERSONAL DATA

7.1 Lawfulness, fairness and transparency.

School will only process personal data where one of the 6 lawful bases (as set out below) has been identified 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 (i.e. DfE census information)
- The data needs to be processed to ensure the vital interests of the individual or another person (i.e. to protect someone's life by collecting data about food allergies or medical conditions)
- The data needs to be processed so that the school, as a public authority, can perform a task in the public interest or exercise its official authority (i.e. to support pupil learning, to monitor and report on pupil attainment progress, to provide appropriate pastoral care and to assess the quality of services)
- The data needs to be processed for the legitimate interests of the school (where the processing is not for any tasks the school performs as a public authority) 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, school will also meet one of the special category conditions for processing under data protection law.

School will always consider the fairness of any data processing. School will ensure it does not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

7.2 Limitation, minimisation and accuracy.

- School will only collect personal data for specified, explicit and legitimate reasons.
- If school needs to use personal data for reasons other than those given when first obtained, school will inform the individuals concerned, and seek consent where necessary.
- Staff must only process personal data where it is necessary in order to do their jobs.
- School will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.
- In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or disposed of securely. This will be done in accordance with the school's record retention schedule.

## 8. SHARING PERSONAL DATA

8.1 School will not normally share personal data with anyone else without consent, but there are certain circumstances where it may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of staff at risk
- School needs to liaise with other agencies – consent will be requested as necessary before doing this
- School suppliers or contractors need data for the provision of services to staff and pupils – for example, IT companies. When doing this, school will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data shared
    - Only share data that the supplier or contractor needs to carry out their service

8.2 School will also share personal data with law enforcement and government bodies where legally required to do so.

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

## 9. ARTIFICIAL INTELLIGENCE (AI) AND DATA PROTECTION

9.1 The school recognises the growing role of Artificial Intelligence (AI) in education, including tools used for learning analytics, assessment support, administrative automation, and safeguarding monitoring. Where AI systems are used, the school is committed to ensuring that personal data is processed lawfully, fairly, and transparently in line with the UK GDPR, the Data Protection Act 2018, and the Data (Use and Access) Act 2025.

9.2 Where AI is used to make decisions that have a legal or significant impact on individuals (such as automated flagging or recommendations), the school will:

- Ensure appropriate human oversight is in place and that decisions are not made solely by automated means without safeguards.
- Inform individuals (or parents/carers, where appropriate) when AI-driven decision-making are used and provide meaningful information about how it works.
- Enable individuals to request human intervention, express their views, and challenge outcomes where automated decisions affect them.
- Complete Data Protection Impact Assessments (DPIAs) for all high-risk AI applications to assess and mitigate risks to privacy and rights.

9.3 Generative tools such as ChatGPT and Google Bard, are increasingly accessible and widely used by staff, pupils, and parents/carers. North Ridge acknowledges the educational potential of these tools but also recognises the associated risks, particularly in relation to the handling of personal and sensitive data.

9.4 To protect the security and confidentiality of such data, individuals are strictly prohibited from inputting personal, sensitive, or confidential information into any unauthorised generative AI tool or chatbot.

9.5 Any instance where personal or sensitive data is entered into an unauthorised AI tool will be treated as a data breach. In such cases, North Ridge will respond in accordance with its established personal data breach procedures.

9.6 The school will only work with AI service providers who can demonstrate compliance with UK data protection law, including the Age Appropriate Design Code when processing children's data.

## 10. BIOMETRIC RECOGNITION SYSTEMS

10.1 Where the school uses biometric recognition systems (e.g. fingerprint or facial recognition technology to access services such as cashless catering or library systems), we will comply with all relevant data protection legislation, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Protection of Freedoms Act 2012, and updates introduced by the Data (Use and Access) Act 2025.

**Definition**

Biometric data is classed as a special category of personal data under the UK GDPR when it is used for the purpose of uniquely identifying an individual through automated processing.

10.2 **Consent and Notification** Before collecting or processing any biometric data from a pupil, the school will:

- Inform parents/carers in writing about the proposed use of biometric data and how it will be used
- Obtain written consent from at least one parent or carer
- Not collect or process any biometric data from a pupil without this prior consent

10.3 Consent can be withdrawn at any time by the parent, carer, or the pupil themselves (if they are capable of understanding the implications). If consent is withdrawn, the school will promptly delete the relevant biometric data.

**10.4 Pupil Refusal**

As required by the Protection of Freedoms Act 2012, if a pupil objects to the use of their biometric data either verbally or non-verbally the school will not process it, even if parental consent has been given.

**10.5 Alternatives to Biometric Systems**

Pupils and staff who choose not to use the biometric system will be provided with an alternative method to access the relevant service (e.g. PIN entry, ID card, or manual payment system).

**10.6 Use of Biometrics for Adults**

Where biometric systems are used for staff or other adults (e.g. for access control or time management), the school will also:

- Obtain informed and freely given consent before participation
- Offer a reasonable alternative method of access if consent is not given or later withdrawn
- Delete biometric data upon withdrawal of consent or when it is no longer required

**10.7 Security and Retention**

All biometric data will be securely stored and protected from unauthorised access. It will only be retained for as long as is necessary to fulfil the purpose for which it was collected, and securely deleted thereafter, in accordance with the school's data retention policy.

## 11. CCTV

11.1 The school uses CCTV in various locations around the school site to ensure it remains safe and complies with the ICO's guidance for the use of CCTV, and comply with data protection principles.

11.2 We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

11.3 Any enquiries about the CCTV system should be directed to Jason Pilling, IT Manager.

## 12. PHOTOGRAPHS AND VIDEOS

12.1 As part of school activities and celebrations, the school may take photographs or record videos of pupils and staff within the school setting.

**12.2** Written consent will be sought from parents/carers before capturing or using images of their child for communication, marketing, or promotional purposes. This will clearly explain how each photograph or video w ll be used to both the parent/carer and the pupil.

**12.3 Use by Parents/Carers -** Photographs or videos taken by parents/carers during school events for personal use are not covered by data protection law. However, to protect the privacy and safety of all pupils, we ask that such images are not shared publicly (e.g., on social media) if they include other children, unless consent has been obtained from all relevant parents/carers (or pupils, where appropriate).

**12.4 School Use of Images** Photographs and videos taken by the school may be used for purposes such as:

- Displaying within the school, including on notice boards, newsletters, brochures, or magazines
- Use by external agencies (e.g., official school photographers, local media, educational campaigns)
- Publishing on the school's website or official social media platforms

12.5 Consent may be withdrawn at any time. Upon withdrawal of consent, the school will stop using the relevant photograph or video and will delete it where reasonably possible.

12.6 To safeguard pupil identity, we will not include full names or other identifiable personal information alongside images without specific consent.

For further details, please refer to our Safeguarding Policy.

## 13. DATA SECURITY AND STORAGE OF RECORDS

13.1 School 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:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices

## 14. DISPOSAL OF RECORDS

14.1 Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely. School may also use a third party to safely dispose of records. Any third party will be required to provide sufficient guarantees that it complies with data protection law.

## 15. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

15.1 Subject access requests.

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request in any form they must immediately forward it to the DPO.

15.2 Children and subject access requests.

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or

carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

15.3 Responding to subject access requests.

15.4 When responding to requests, school:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

15.5 School may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

15.6 If the request is unfounded or excessive, school may refuse to act on it, or charge a reasonable fee to cover administrative costs.

15.7 School will also take into account whether the request is repetitive in nature when making this decision.

15.8 When school refuses a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

## 16. PARENTAL REQUESTS TO SEE THE EDUCATIONAL RECORD

16.1 Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request. All requests must be made in writing to the DPO. The identity of the requestor must be established before the disclosure of any personal information.

16.2 If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

16.3 This right applies as long as the pupil concerned is aged under 18.

16.4 There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

## 17. PERSONAL DATA BREACHES

17.1 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 appropriate procedures and if required we will report the data breach to the ICO within 72 hours after becoming aware of it.

## 18. TRAINING

18.1 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.

## 19. COMPLAINTS

1.1 Any complaint about Data Protection should be referred to the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, Telephone 01625 545700, Website www.ico.org.uk