Data Protection Policy

Policy Information	
Policy Author: A Clewlow Governing Board approval date/date policy is in effect from: Spring 2025	
Review information:	
Approved by:	Intuition School Governing Board

Information		
GDPR Lead/DPO: Sophie White (Office@intuitionschool.co.uk) Principal: Amy Clewlow		
Latest Review information:	**Summary of amendments**	**Date of next review:**
Date: March 2026 Name of reviewer/s: Amy Clewlow	Updated/revised content and added privacy notices	**March 2027**

Data Protection Policy

Contents

1. Aims
2. Legislation and guidance
3. Definitions
4. The data controller
5. Roles and responsibilities
6. Data protection principles
7. Collecting personal data
8. Sharing personal data
9. Subject access requests and other rights of individuals
10. Parental requests to see the educational record
11. Biometric recognition systems
12. CCTV / Surveillance systems
13. Photographs and videos
14. Data protection by design and default
15. Data security and storage of records
16. Retention and disposal of records
17. Personal data breaches
18. Training
19. Monitoring arrangements

Appendix 1: Personal data breach procedure
Appendix 2: Staff Privacy Notice
Appendix 3: Pupil Privacy Notice
Appendix 4: Parent/Carer Privacy Notice
Appendix 5: Governor/Trustee Privacy Notice

1. Aims

Our Organisation is committed to ensuring that all personal data is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

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

We aim to ensure that:

- Individuals' rights are protected
- Data is processed lawfully, fairly and transparently
- Staff understand their responsibilities
- Data is kept secure and only used where necessary

2. Legislation and Guidance

This policy meets the requirements of:

- UK GDPR (retained EU law)
- Data Protection Act 2018
- Education (Pupil Information) (England) Regulations 2005
- Protection of Freedoms Act 2012 (biometric data)
- ICO guidance including:
    - Subject Access Requests (SARs)
    - CCTV code of practice
    - Data sharing guidance

3. 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 ● 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.
Unstructured manual data	Under Section 24 of the Data Protection Act 2018, some paper-based information normally excluded from the definition of personal data is accessible to the right of access and rectification. This essentially refers to handwritten notes.

4. The Data Controller

The Organisation is registered with the Information Commissioner's Office (ICO) as a Data Controller and renews this registration annually.

We determine the purposes and means of processing personal data.

5. Roles and Responsibilities

Governing Board / Proprietor

Responsible for ensuring compliance with UK GDPR and holding the organisation accountable.

Data Protection Officer (DPO)

The DPO:

- Monitors compliance
- Advises on data protection law
- Acts independently
- Is the main contact for the ICO and data subjects
- Oversees breach reporting
- The DPO is responsible for providing advice on DPIAs, monitoring compliance, and acting as contact point for the ICO.

DPO: Sophie White, office@intuitionschool.co.uk

Principal / Senior Leadership Team

Responsible for day-to-day implementation of this policy.

All Staff

All staff must:

- Only access data needed for their role
- Keep data secure at all times
- Report breaches immediately
- Follow all procedures in this policy
- Ensure data is accurate and up to date

Failure to comply may result in disciplinary action.

6. Data Protection Principles

We comply with the UK GDPR principles. Personal data must be:

- Processed lawfully, fairly and transparently
- Collected for specified and legitimate purposes
- Adequate, relevant and limited
- Accurate and up to date
- Kept for no longer than necessary
- Processed securely

7. Collecting Personal Data

7.1 Lawful Basis for Processing

We process data under one or more of the following lawful bases:

- Legal obligation
- Public task
- Contract
- Legitimate interests
- Consent
- Vital interests

The lawful basis applied depends on the nature of the processing activity and is documented in internal records.

If data is not provided:

-Staff: may not be able to enter into or continue employment

-Pupils: may not be able to be admitted or supported effectively

-Parents/carers: may impact safeguarding, communication, or emergency response

7.2 Special Category Data

We apply additional safeguards when processing sensitive data and ensure at least one Article 9 condition is met.

7.3 Transparency

When data is collected, individuals will be informed of:

- Why data is collected
- How it will be used
- Who it may be shared with
- How long it will be kept

Privacy notices are published and reviewed annually.

Where personal data is not collected directly from individuals (e.g. previous schools or Local Authorities), we will provide transparency information within a reasonable period.

7.4 Data Minimisation and Accuracy

We only collect data that is necessary and ensure it is accurate. Staff must update records promptly.

8. Sharing Personal Data

We only share data where lawful and necessary, including:

- Safeguarding concerns
- Legal obligations
- Educational support services
- Approved third-party providers

We ensure:

- Data sharing agreements are in place
- Only necessary data is shared
- Recipients comply with UK GDPR

International Transfers

Data is only transferred outside the UK where adequacy regulations apply or appropriate safeguards (such as IDTAs) are in place. This may include cloud-based educational and administrative systems used by the school.

International transfers may include:

- Microsoft 365 / Google Workspace / MIS (IRIS) / assessment platforms(such as IXL, PASS)

These systems may process and store personal data in the UK and/or EEA in accordance with UK GDPR safeguards.

9. Subject Access Requests and Rights

Individuals have the right to:

- Access their personal data
- Request correction
- Request deletion (where applicable)
- Restrict processing
- Object to processing
- Data portability

Where exercising rights, individuals may be required to provide proof of identity.

9.1 Subject Access Requests (SARs)

We will:

- Respond within 1 month
- Extend to 3 months if complex
- Provide information free of charge (unless excessive)

Requests must include sufficient detail. Staff must forward all SARs to the DPO immediately.

9.2 Children's Rights

Children aged 12+ may exercise rights depending on competence (Gillick competence considered). Parental access may be restricted where appropriate. Where a child is considered competent, their views will be taken into account when responding to requests.

9.3 Refusal of Requests

We may refuse requests that are:

- Manifestly unfounded
- Excessive

Reasons will be explained and individuals may complain to the ICO.

10. Parental Requests for Educational Records

Parents/carers may request access under the Education (Pupil Information) (England) Regulations 2005.

We will:

- Respond within 15 school days
- Provide copies or viewing access
- Charge only reasonable copying costs

Certain information may be withheld if disclosure could cause harm.

11. Biometric Recognition Systems

Where used, we will:

- Obtain written parental consent
- Allow withdrawal at any time
- Provide alternatives
- Delete biometric data when consent is withdrawn

A DPIA and risk assessment will be completed prior to introduction or significant change of any biometric system.

12. CCTV / Surveillance

We use CCTV to maintain safety and security.
We ensure:

- Clear signage is displayed
- Recordings are securely stored
- Access is restricted
- Footage is retained only as long as necessary

A DPIA will be completed prior to installation or significant changes to CCTV systems.

13. Website, cookies and digital monitoring

The school website may collect personal data when users complete forms, contact the school, or interact with online content. This data is processed in line with this policy and used only for the stated purpose.

Cookies

Cookies are small files stored on your device to help the website function and improve user experience.

We use:

- **Essential cookies** – required for the website to operate (no consent needed)
- **Analytics cookies** – help us understand website usage (only used with consent)
- **Functional cookies** – remember user preferences where applicable

Users can accept or reject non-essential cookies and change preferences at any time via browser or website settings.

Non-essential cookies will only be used with user consent.

Third-party services

The website may contain links or embedded content (e.g. videos, maps, learning platforms). These providers may set their own cookies and collect data independently. Users should check their privacy policies.

Analytics

Where used, analytics data is aggregated and does not directly identify individuals. It is used to improve website performance and user experience.

14. Photographs and Videos

We:

- Obtain consent where required
- Explain use clearly
- Allow withdrawal of consent
- Do not publish unnecessary identifying information

15. Data Protection by Design and Default

Systems and processes are configured to ensure privacy by default, meaning only the minimum necessary data is collected, accessed, and retained unless further processing is justified and authorised.

DPIAs will be carried out for any new system, process or significant change involving personal data.

We integrate data protection into all processes by:

- Minimising data collection
- Ensuring security is built into systems
- Conducting DPIAs where high risk exists

DPIAs

Required when:

- Introducing new technology
- Processing sensitive data at scale
- Monitoring individuals systematically

16. Data Security and Storage

We implement robust security measures including:

- Locked storage for paper records
- Encrypted digital systems
- Strong passwords (12+ characters or passphrases)
- Multi-factor authentication where possible
- Secure transport of data off-site

Staff must not leave confidential data unattended.

17. Retention and Disposal of Records

We follow the IRMS Records Retention Schedule.

Data is:

- Kept only for required periods
- Reviewed regularly
- Securely destroyed when no longer needed

Retention periods are reviewed regularly to ensure continued compliance with the IRMS Records Management Toolkit.

18. Personal Data Breaches

In the event of a breach:

- It is reported immediately to the DPO
- Investigations are carried out
- ICO notified within 72 hours where required
- Affected individuals are informed if risk is high

All breaches will be assessed in line with UK GDPR Articles 33 and 34 to determine notification requirements.

19. Training

All staff receive:

- Induction training
- Regular updates at team briefings
- Annual mandatory GDPR and data protection training is provided to all staff, with additional updates issued where legislation, systems or risks change. Training is mandatory for all staff and is recorded and monitored for compliance.

20. Monitoring and Review

The DPO monitors compliance.
This policy is reviewed every 2 years or sooner if required.

APPENDICES

APPENDIX 1: PERSONAL DATA BREACH PROCEDURE

1. Purpose

This procedure outlines the school's response to any personal data breach to ensure compliance with UK GDPR Articles 33 and 34, and guidance from the Information Commissioner's Office (ICO).

A personal data breach is defined as:

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

This includes:

- Loss of paper records
- Sending data to the wrong recipient
- Cybersecurity incidents (phishing, hacking, ransomware)
- Unauthorised access to systems or files
- Theft or loss of devices containing personal data

2. Immediate Actions (Containment Stage)

All staff must:

- Report suspected breaches immediately to the Headteacher / Data Protection Lead
- Take immediate steps to contain the breach where safe to do so:
    - Recall emails (if possible)
    - Secure or isolate affected systems/devices
    - Retrieve misdirected documents if possible
    - Change passwords if compromise suspected
- Do not attempt to investigate independently beyond containment

3. Initial Assessment

The Data Protection Lead (or DPO) will:

- Confirm whether a breach has occurred
- Identify the type of data involved (special category, financial, pupil, staff, etc.)
- Establish:
    - What data was involved
    - Number of individuals affected
    - Whether data is still accessible or has been recovered
    - Likelihood and severity of harm

4. Risk Assessment

Each breach will be assessed for risk to individuals, including:

- Identity theft or fraud risk
- Safeguarding risks (especially for pupils)
- Financial risk
- Emotional distress or reputational harm

A breach is considered **reportable to the ICO** if it is likely to result in a risk to individuals' rights and freedoms.

Where a breach is assessed as likely to result in a high risk to individuals, the DPO will determine whether notification to affected individuals is mandatory under Article 34 UK GDPR. The DPO will determine whether

the breach is likely to result in a risk or high risk to individuals and whether ICO and/or data subject notification is required.

5. Notification to the ICO (within 72 hours)

Where required, the school will notify the ICO without undue delay and within **72 hours** of becoming aware of the breach.

The report will include:

- Nature of the breach
- Categories and approximate number of individuals affected
- Likely consequences
- Measures taken or proposed to address the breach
- Contact details of the Data Protection Lead

If full details are not yet known, initial notification will still be made and updated as further information becomes available.

6. Notification to Individuals

Where a breach is likely to result in **high risk to individuals**, the school will inform affected individuals without undue delay.

Communication will include:

- Description of the breach
- What data was involved
- Potential consequences
- Actions taken by the school
- Advice on steps individuals should take
- Contact details for further support

Safeguarding considerations will be prioritised when notifying parents/carers.

7. Documentation

All breaches will be recorded in a **Data Breach Log**, including:

- Date and time of breach
- Nature of incident
- Data involved
- Individuals affected
- Actions taken
- ICO notification decision
- Outcome and lessons learned

This record is retained for accountability and audit purposes.

8. Review and Preventative Action

Following any breach, the school will:

- Conduct a full post-incident review
- Identify root causes

- Implement corrective actions (training, system changes, policy updates)
- Update risk assessments and DPIAs if necessary
- Share learning with relevant staff

9. Staff Responsibility

All staff are responsible for:

- Handling data securely
- Reporting breaches immediately
- Completing mandatory GDPR training
- Following secure communication protocols

Failure to report a breach may result in disciplinary action.

APPENDIX 2: STAFF PRIVACY NOTICE

1. Introduction

The school is the Data Controller for staff personal data. This notice explains how we collect, use, and protect your information in line with UK GDPR and the Data Protection Act 2018.

2. Why we collect staff data

We process staff data to:

- Fulfil employment contracts
- Pay salary and pensions
- Manage HR administration
- Ensure safeguarding compliance
- Conduct recruitment and vetting
- Support performance management
- Provide training and CPD
- Meet legal and regulatory obligations

3. Categories of data collected

We may receive personal data from previous schools/employers, Local Authorities, health professionals, or other agencies.

We may process:

- Identification data (name, address, DOB, contact details, NI number)
- Employment data (role, contract terms, attendance, absence)
- Payroll and tax information
- Safeguarding and recruitment data (DBS checks, references, right to work)
- Health data (occupational health, fitness to work, reasonable adjustments where disclosed)
- Disciplinary or capability records (where applicable)

4. Lawful basis for processing

We process staff data under:

- Contract (Article 6(1)(b))
- Legal obligation (Article 6(1)(c))
- Public task (Article 6(1)(e))

Special category data is processed under:

- Employment law obligations (Article 9(2)(b))
- Substantial public interest (Article 9(2)(g))

5. Data sharing

We may share staff data with:

- HMRC
- Pension providers
- Payroll providers

- Occupational health services
- Department for Education (DfE) / Local Authority
- DBS service providers
- IT, HR and MIS system providers

All sharing is subject to appropriate contractual and data protection safeguards.

6. Data retention

We retain data in line with statutory guidance:

- Personnel records: typically 6 years after employment ends
- Payroll records: minimum 6 years
- Recruitment records: 6–12 months unless required longer
- Safeguarding records: retained in line with safeguarding requirements

7. Your rights

You have the right to:

- Access your data
- Rectify inaccurate data
- Restrict processing
- Object to processing
- Request erasure (where applicable)

Requests will be responded to within 1 calendar month.

8. Security

We protect staff data through:

- Secure HR systems
- Password protection and multi-factor authentication (where available)
- Restricted access controls
- Encryption
- Secure disposal of records

9. Complaints

If you have concerns about how your data is handled, you should contact the school's Data Protection Lead in the first instance.

You also have the right to complain to the Information Commissioner's Office (ICO):
https://ico.org.uk/make-a-complaint/

APPENDIX 3: PUPIL PRIVACY NOTICE

1. Purpose of processing

We collect and use pupil data to:

- Deliver education and learning
- Track progress and attainment
- Safeguard children
- Meet statutory reporting requirements
- Provide SEN and pastoral support
- Manage school administration

2. Types of pupil data

We may receive personal data from previous schools, Local Authorities, health professionals, or other agencies.

We may process:

- Personal identification details
- Attendance and behaviour records
- Assessment and exam results
- SEN and EHCP information
- Medical and health information
- Safeguarding and welfare records
- Photographs and video (where consent applies)

3. Lawful basis

We process pupil data under:

- Legal obligation (Article 6(1)(c))
- Public task (Article 6(1)(e))

Special category data is processed under:

- Substantial public interest
- Health and social care purposes
- Safeguarding obligations

4. Sharing pupil data

We may share with:

- Department for Education (DfE) and Local Authority
- Exam boards
- NHS and health professionals
- Social care and safeguarding partners
- Next schools or alternative provision
- Approved digital learning platforms

Only the minimum necessary data is shared.

5. Retention

- Educational records: typically until age 25
- Safeguarding records: retained in line with legal requirements (often longer)
- SEN records: retained as part of the educational record

6. Rights

Parents and pupils (where appropriate) have the right to:

- Access data
- Rectify inaccurate data
- Restrict processing
- Object to processing

7. Safeguarding

Where safeguarding concerns exist:

- Information may be shared without consent
- Legal obligations override confidentiality

8. Complaints

If you have concerns about how your data is handled, please contact the school's Data Protection Lead in the first instance.

You also have the right to complain to the Information Commissioner's Office (ICO):
https://ico.org.uk/make-a-complaint/

APPENDIX 4: PARENT/CARER PRIVACY NOTICE

1. Purpose

We process parent/carer data to support:

- Communication between school and home
- Safeguarding and welfare
- Admissions and school administration
- Attendance monitoring
- Emergency contact arrangements

2. Data collected

We may receive personal data from previous schools, Local Authorities, health professionals, or other agencies.

We may process:

- Names and contact details
- Relationship to pupil
- Emergency contact information
- Communication records
- Consent preferences

3. Lawful basis

We process parent/carer data under:

- Public task
- Legal obligation
- Legitimate interests (communication and administration)

4. Data sharing

We may share data with:

- Local Authority
- Safeguarding partners
- Transport providers (where applicable)
- IT and communication systems

We do not sell or misuse personal data.

5. Retention

Data is retained only for as long as necessary for:

- Active schooling period
- Safeguarding requirements
- Legal and statutory obligations

6. Rights

You have the right to:

- Access your data
- Correct inaccurate data
- Restrict processing
- Object to processing

7. Complaints

If you have concerns about how your data is handled, please contact the school's Data Protection Lead in the first instance.

You also have the right to complain to the Information Commissioner's Office (ICO):
https://ico.org.uk/make-a-complaint/

APPENDIX 5: GOVERNOR / TRUSTEE PRIVACY NOTICE

1. Purpose

We process governor/trustee personal data to:

- Support governance and statutory accountability
- Maintain records of board membership and eligibility
- Ensure compliance with education and safeguarding legislation
- Manage DBS and vetting requirements
- Support governance communication and operations

2. Data collected

We may receive personal data from Local Authorities, the Department for Education, or other relevant bodies.

We may process:

- Name and contact details
- Appointment details and term of office
- DBS and vetting information
- Declaration of interests
- Attendance records
- Training and induction records

3. Lawful basis

We process governor/trustee data under:

- Legal obligation (Article 6(1)(c))
- Public task (Article 6(1)(e))

Special category data is processed under:

- Substantial public interest (safeguarding and governance compliance)

4. Data sharing

We may share data with:

- Department for Education (GIAS – Get Information About Schools)
- Local Authority
- Safeguarding partners
- IT systems used for governance and administration

All sharing is subject to appropriate data protection safeguards.

5. Retention

We retain governance data in line with statutory requirements:

- Governance records: retained for audit and accountability purposes (often 6 years or longer)
- DBS information: retained in line with safer recruitment guidance

- Minutes, registers and declarations: retained long-term or permanently for governance accountability

6. Rights

You have the right to:

- Access your data
- Rectify inaccurate data
- Restrict processing
- Object to processing (where applicable)

Requests will be responded to within 1 calendar month.

7. Complaints

If you have concerns about how your data is being handled, please contact the school's Data Protection Lead in the first instance.

You also have the right to complain to the Information Commissioner's Office (ICO):
https://ico.org.uk/make-a-complaint/