DATA PROTECTION POLICY

This policy applies to the whole school

The Policy is available to the school staff on the 'Staff Shared'

We have a whole school approach to safeguarding, which is the golden thread that runs throughout every aspect of Landon school. All our school policies support our approach to safeguarding (pupil protection). Our fundamental priority is our pupils and their wellbeing; this is first and foremost.

Scope: All who work, volunteer or supply services to our school have an equal responsibility to understand and implement this policy and its procedures both within and outside of normal school hours, including activities away from school. All new employees and volunteers are required to state that they have read, understood and will abide by this policy and its procedural documents and confirm this via the signing of their employment contract.

Legal Status: Complies with The Education (Independent School Standards) (England) Regulations currently in force. Monitoring and Review: These arrangements are subject to continuous monitoring, refinement, and audit by the Headteacher. The Proprietor and Advisory Board will undertake a full annual review of this document, inclusive of its implementation and the efficiency with which the related duties have been implemented. This review will be formally documented in writing. Any deficiencies or weaknesses recognised in arrangements or procedures will be remedied immediately and without delay. All staff will be informed of the updated/reviewed arrangements and it will be made available to them in writing or electronically.

Policy Agreed: October 2025
Date Published: October 2025
Next Review: October 2027

Signed:

J. Tranter	A Thompson	K. Thompson
Mr Jody Tranter Headteacher	Mr Andy Thompson Proprietor who is the Chair of the Advisory Board	Katie Thompson Proprietor's agent

Contents

14. Privacy Notices
15. Data Protection Impact Assessments (DPIAs)
16. Data Breaches
17. Training and Awareness
18. Appendices

1. Introduction and Purpose

Landon School is committed to protecting the privacy and security of personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

As a special educational needs school for autistic children, we process significant amounts of personal data, including special category data relating to health, special educational needs, and safeguarding. This policy sets out how we handle this data responsibly, transparently, and in compliance with the law.

1.1 Purpose of This Policy

This policy aims to:

- Ensure compliance with UK GDPR and DPA 2018
- Protect the rights and privacy of data subjects (pupils, parents, staff, and others)
- Establish clear procedures for data handling, security, and breach management
- Define roles and responsibilities for data protection
- Promote good data protection practice across the school
- Provide transparency about our data processing activities

1.2 Legal Framework

This policy is based on the following legislation:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Education Act 1996
- Freedom of Information Act 2000
- Protection of Freedoms Act 2012
- Equality Act 2010
- Children and Families Act 2014

2. Definitions

Term	Definition

Personal Data	Any information relating to an identified or identifiable individual (data subject). This includes names, addresses, identification numbers, location data, online identifiers, or factors specific to their physical, physiological, genetic, mental, economic, cultural, or social identity.
Special Category Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life, or sexual orientation. This data requires additional protection.
Processing	Any operation performed on personal data, including collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, restriction, erasure, or destruction.
Data Subject	The individual to whom personal data relates (e.g., pupil, parent, staff member).
Data Controller	The organisation (Landon School) that determines the purposes and means of processing personal data.
Data Processor	A third party that processes personal data on behalf of the data controller (e.g., cloud storage providers, payroll services).
Data Protection Officer (DPO)	The person responsible for overseeing data protection compliance within the school.
Data Breach	A security incident that leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

3. Data Protection Principles

Landon School adheres to the seven key principles of UK GDPR. All personal data must be:

1. **Processed lawfully, fairly, and transparently** - We have a valid legal basis for processing data and are transparent about how we use it.

2. **Collected for specified, explicit, and legitimate purposes** - We are clear about why we collect data and do not use it for incompatible purposes.
3. **Adequate, relevant, and limited to what is necessary** - We only collect and process data that is needed for our specified purposes.
4. **Accurate and kept up to date** - We take reasonable steps to ensure data accuracy and correct or delete inaccurate data promptly.
5. **Kept for no longer than necessary** - We retain data only as long as required and follow our retention schedule for deletion.
6. **Processed securely** - We implement appropriate technical and organisational measures to protect data from unauthorised or unlawful processing, accidental loss, destruction, or damage.
7. **The controller is accountable** - We can demonstrate compliance with these principles through documentation, policies, and regular reviews.

4. Roles and Responsibilities

4.1 The Proprietor (Mr Andy Thompson)

The Proprietor has overall responsibility for ensuring that the school complies with data protection legislation and is accountable for:

- Ensuring sufficient resources are allocated for data protection compliance
- Approving this policy and significant amendments
- Ensuring the appointment of a competent Data Protection Officer
- Overseeing the school's data protection strategy

4.2 The Headteacher (Mr Jody Tranter)

The Headteacher is responsible for:

- Implementing this policy and ensuring staff compliance
- Acting as the key contact for data protection matters
- Ensuring staff receive appropriate data protection training
- Reporting data protection issues to the Proprietor and DPO
- Ensuring data protection is embedded in school culture
- Making decisions on subject access requests and individual rights requests

4.3 The Data Protection Officer (DPO)

Landon School has appointed a Data Protection Officer who is responsible for:

- Informing and advising the school about data protection obligations
- Monitoring compliance with UK GDPR and DPA 2018
- Providing advice on Data Protection Impact Assessments (DPIAs)
- Acting as the contact point for data subjects and the Information Commissioner's Office (ICO)
- Conducting regular data protection audits
- Maintaining the Record of Processing Activities
- Investigating data breaches and recommending remedial action

DPO Contact Details:
Jarka Sekhon, School Business Manager, 0208 153 0201
Email: dpo@landonschool.co.uk

4.4 All Staff Members

Every member of staff has a responsibility to:

- Process personal data only in accordance with this policy and training
- Ensure data is accurate, secure, and kept confidential
- Only access personal data necessary for their role
- Report any data protection concerns or breaches immediately
- Complete mandatory data protection training
- Follow the school's IT security policies and password procedures
- Not share login credentials or leave computers unlocked
- Be vigilant against phishing and social engineering attempts

4.5 Third-Party Data Processors

Any organisation processing personal data on behalf of Landon School must:

- Sign a data processing agreement before processing begins
- Process data only on documented instructions from the school
- Implement appropriate security measures
- Not sub-contract processing without written authorisation
- Assist with subject access requests and data breaches
- Delete or return data at the end of the contract

5. Lawful Basis for Processing

Before processing personal data, the school identifies and documents the lawful basis under UK GDPR Article 6. We rely on the following lawful bases:

5.1 Public Task (Primary Basis)

Most of our data processing is carried out under the public task basis, as we are exercising official authority as an independent special educational needs school providing education and care to autistic children.

Examples include:

- Maintaining pupil records and educational progress data
- Delivering the curriculum and pastoral care
- Safeguarding and child protection
- Meeting special educational needs
- Managing staff employment and payroll

5.2 Legal Obligation

We process data to comply with legal obligations, including:

- Statutory reporting to the Department for Education

- Sharing information for safeguarding purposes
- Health and safety obligations
- Employment law requirements
- Equality Act duties

5.3 Vital Interests

In rare circumstances, we may process data to protect someone's life, such as:

- Medical emergencies
- Immediate safeguarding concerns

5.4 Legitimate Interests

Where appropriate, we may rely on legitimate interests for:

- Marketing school events to current parents
- Alumni communications (with opt-out options)
- CCTV for security purposes

Before relying on legitimate interests, we conduct a Legitimate Interests Assessment to ensure our interests are not overridden by the individual's rights and freedoms.

5.5 Consent

We obtain explicit consent for:

- Use of pupil photographs on the website and social media
- Biometric data collection (if applicable)
- Non-essential communications
- Some educational trips or activities
- Marketing to prospective parents

Consent must be freely given, specific, informed, and unambiguous. Individuals can withdraw consent at any time, and we make this process as easy as giving consent.

6. Special Category Data and Criminal Offence Data

6.1 Special Category Data

As a special needs school for autistic children, we regularly process special category data including:

- Health data (medical conditions, medication, therapy records)
- Special educational needs information
- Genetic and biometric data (if used)
- Racial or ethnic origin
- Religious beliefs

In addition to a lawful basis under Article 6, we must have a condition for processing under Article 9. We primarily rely on:

Article 9(2)(b) - Employment, social security, and social protection

For processing staff health data and managing sickness absence.

Article 9(2)(g) - Substantial public interest

Under Schedule 1, Part 2 of the DPA 2018, particularly:

- Paragraph 6: Statutory and government purposes
- Paragraph 18: Safeguarding of children and individuals at risk

Article 9(2)(h) - Health and social care

For processing health data to provide education and care services.

6.2 Appropriate Policy Document

Where we rely on substantial public interest conditions, we maintain an Appropriate Policy Document (see Appendix B) that:

- Documents our procedures for complying with data protection principles
- Explains our policies for retaining and erasing special category data
- Is reviewed at least annually

6.3 Criminal Offence Data

We may process criminal offence data for safeguarding purposes or as part of staff recruitment (DBS checks). This is processed under:

- Legal obligation (DBS checks)
- Substantial public interest (safeguarding)

7. Pupil Data

7.1 Categories of Pupil Data We Process

We collect and process the following categories of pupil data:

- **Personal identifiers:** Name, date of birth, address, contact details, photographs
- **Educational data:** Academic progress, attainment, curriculum records, attendance, behaviour
- **Special educational needs:** Autism diagnosis, Education Health and Care Plans (EHCPs), assessments, support plans, therapy records
- **Medical and health:** Medical conditions, medication, dietary requirements, allergies, GP details
- **Safeguarding:** Concerns, referrals, meeting records, risk assessments
- **Family information:** Parent/carer details, parental responsibility, family circumstances
- **Financial:** Free school meal eligibility, trip payments
- **Biometric data:** Only if used and with explicit parental consent

7.2 Sources of Pupil Data

We obtain pupil data from:

- Parents and carers
- Previous schools and educational settings
- Local authorities and commissioning bodies
- Healthcare professionals and therapists
- Social care services

- The pupil themselves (where appropriate)

7.3 Why We Use Pupil Data

We use pupil data to:

- Provide appropriate education and support for autistic children
- Monitor and report on pupil progress
- Provide pastoral and medical care
- Keep children safe (safeguarding)
- Assess the quality of our services
- Comply with legal obligations and statutory reporting
- Manage school operations (admissions, timetabling, communication)

7.4 Pupil Rights

Pupils have the same data protection rights as adults. However, the school may need to consider the child's age and understanding when responding to rights requests.

For pupils aged 12 and under, parents/carers typically exercise rights on their behalf. For pupils aged 13-18, we assess competence on a case-by-case basis.

8. Staff Data

8.1 Categories of Staff Data We Process

- **Personal details:** Name, address, contact details, date of birth, national insurance number
- **Employment:** Job title, contract type, salary, bank details, pension, absence records
- **Recruitment:** Application forms, references, interview notes, DBS checks
- **Performance:** Appraisals, capability records, training records
- **Health:** Sickness absence, occupational health referrals, reasonable adjustments
- **Disciplinary:** Records of investigations, warnings, dismissals
- **Emergency contacts:** Next of kin details

8.2 Why We Use Staff Data

- To fulfil the employment contract
- To meet legal obligations (taxation, pension, safeguarding)
- To manage performance and professional development
- To ensure health and safety
- To process payroll and benefits

8.3 Sharing Staff Data

We may share staff data with:

- HMRC and pension providers
- The Disclosure and Barring Service
- Occupational health services
- Professional advisers (legal, HR, payroll)
- Employment tribunals or courts (if required)

9. Data Sharing and Third-Party Processing

9.1 Who We Share Data With

Landon School may share personal data with:

- **Local authorities:** For EHCP reviews, safeguarding, statutory reporting
- **Department for Education (DfE):** Statutory school census data
- **Healthcare professionals:** GPs, therapists, CAMHS (with consent or legal basis)
- **Social care services:** For safeguarding and child protection
- **Police and courts:** Where legally required
- **Educational psychologists and SEND services**
- **Transport providers:** For school transport arrangements
- **IT service providers:** Cloud storage, MIS systems (with data processing agreements)
- **Ofsted:** During inspections
- **Professional advisers:** Legal, HR, payroll (with data processing agreements)

9.2 Data Processing Agreements

Before sharing data with any third-party processor, we ensure:

- A written data processing agreement is in place
- The processor provides sufficient guarantees of security
- The processor processes data only on our documented instructions
- The processor notifies us of any data breaches
- The contract includes terms for data deletion or return at contract end

9.3 International Transfers

We do not routinely transfer personal data outside the UK. If an international transfer becomes necessary, we will:

- Ensure the country has an adequacy decision from the UK Government, OR
- Implement appropriate safeguards (e.g., standard contractual clauses), OR
- Obtain explicit consent where no other safeguard is available

9.4 Department for Education (DfE) Data Sharing

The DfE collects personal data from schools via statutory data collections. We are required by law to provide information to the DfE as part of these collections.

Some of this data is then shared with local authorities and NHS England. For more information about DfE data sharing, see:

https://www.gov.uk/education/data-collection-and-censuses-for-schools

10. Data Security and Storage

10.1 Security Measures

Landon School implements appropriate technical and organisational measures to protect personal data, including:

Technical Measures:

- Password-protected computers and encrypted devices
- Secure cloud storage with encryption at rest and in transit
- Regular software updates and patches
- Firewall and anti-virus protection
- Multi-factor authentication for sensitive systems
- Regular backups stored securely
- Email filtering for phishing and malware

Organisational Measures:

- Access controls - staff only access data necessary for their role
- Clear desk policy for paper records
- Locked filing cabinets for sensitive paper records
- Secure disposal of paper records (cross-cut shredding)
- Visitor sign-in procedures and restricted access to office areas
- Staff training on data protection and security
- Disciplinary procedures for security breaches

10.2 Password Policy

All staff must:

- Use strong, unique passwords (minimum 8 characters, mix of upper/lower case, numbers, symbols)
- Not share passwords or write them down
- Change passwords every 90 days or immediately if compromised
- Not use the same password for multiple accounts
- Lock computers when away from desks

10.3 Working Remotely

When working remotely, staff must:

- Only use school-approved devices and systems
- Connect via secure, encrypted connections (VPN if provided)
- Not use personal email accounts for school business
- Ensure physical security of devices and documents
- Not allow family members to access school systems or data

10.4 Paper Records

Paper records containing personal data must be:

- Stored in locked filing cabinets when not in use
- Not left unattended on desks or in open areas
- Transported securely in sealed envelopes or locked bags

- Destroyed by cross-cut shredding when no longer needed

10.5 Email and Communication Security

When emailing personal data:

- Check recipient addresses carefully before sending
- Use BCC for bulk emails to protect email addresses
- Encrypt sensitive attachments or use secure file transfer
- Do not send special category data unless absolutely necessary and secure
- Be aware of phishing attempts - verify unexpected requests for data

11. Data Retention and Deletion

11.1 Retention Principles

We only retain personal data for as long as necessary for the purposes for which it was collected. Retention periods are based on:

- Legal and regulatory requirements
- Operational needs
- Best practice guidance

11.2 Retention Schedule

Landon School follows this retention schedule (see Appendix C for full schedule):

Record Type	Retention Period	Action After Retention
Pupil educational records	25 years from date of birth	Secure destruction
EHCP and SEND records	25 years from date of birth	Secure destruction
Safeguarding records	25 years from date of birth or 7 years from last entry (whichever is longer)	Secure destruction
Pupil attendance registers	Current year + 3 years	Secure destruction
Staff personnel files	Termination + 6 years	Secure destruction

Recruitment records (unsuccessful)	6 months from decision	Secure destruction
DBS certificates	6 months after verification	Secure destruction
Payroll records	Current year + 6 years	Secure destruction
Accident reports	Date of incident + 21 years (adults) 25 years from date of birth (children)	Secure destruction
CCTV footage	30 days (unless required for investigation)	Secure deletion

11.3 Secure Deletion

When data reaches the end of its retention period, it must be securely deleted:

- **Paper records:** Cross-cut shredding or confidential waste disposal
- **Electronic records:** Secure deletion software or physical destruction of devices
- **Cloud storage:** Permanent deletion including backups
- **Devices:** Factory reset or secure wiping before disposal/reuse

12. Individual Rights

Under UK GDPR, individuals have the following rights regarding their personal data:

12.1 Right to Be Informed

Individuals have the right to know how their data is processed. We provide this through privacy notices (see Section 14).

12.2 Right of Access (Subject Access Request)

Individuals have the right to access their personal data. See Section 13 for our SAR procedure.

12.3 Right to Rectification

Individuals can request correction of inaccurate or incomplete data. We will:

- Respond within one month
- Correct the data if inaccurate
- Notify third parties who received the data (where appropriate)

12.4 Right to Erasure ('Right to Be Forgotten')

Individuals can request deletion of their data in certain circumstances. However, this right is limited where we have a legal obligation to retain data (e.g., safeguarding records, statutory reporting).

We will consider each request on a case-by-case basis and balance the individual's rights against our legal obligations.

12.5 Right to Restrict Processing

Individuals can request we stop processing their data (but not delete it) in certain circumstances, such as while disputing accuracy.

12.6 Right to Data Portability

Where processing is based on consent or contract and carried out by automated means, individuals can request their data in a commonly used electronic format.

12.7 Right to Object

Individuals can object to processing based on legitimate interests or for direct marketing purposes. We will stop processing unless we have compelling legitimate grounds that override the individual's rights.

12.8 Rights Related to Automated Decision-Making

Landon School does not use automated decision-making or profiling. If this changes, individuals will have the right to human review of decisions.

13. Subject Access Requests (SARs)

13.1 What is a SAR?

A Subject Access Request is a request from an individual to access their personal data held by the school.

13.2 How to Make a SAR

Requests should be made in writing (email or letter) to:

Headteacher: **Mr** **Jody** **Tranter**
Email: head@landonschool.co.uk
Address: Landon School, Aviation House
Harmondsworth Lane
Harmondsworth
West Drayton UB7 0LQ

13.3 Responding to SARs

We will:

1. **Verify identity:** Request proof of identity (photographic ID) to prevent unauthorized disclosure
2. **Clarify request:** Contact the requester if the request is unclear or too broad
3. **Search for data:** Conduct thorough searches across all systems and locations
4. **Consider exemptions:** Assess whether any exemptions apply (e.g., data about third parties)

5. **Provide response:** Supply copies of personal data in a commonly used electronic format (or hard copy if preferred)

13.4 Timescales and Fees

- **Response time:** Within one month of receipt of request (can be extended by two months for complex requests)
- **Fee:** Free of charge (unless request is manifestly unfounded or excessive)

13.5 Educational Records

Parents have a separate right to access their child's educational record under the Education (Pupil Information) (England) Regulations 2005. These requests must be responded to within 15 school days.

13.6 Third-Party Information

Where data includes information about third parties (e.g., other pupils, staff members), we will:

- Redact third-party information unless they consent to disclosure
- Consider whether disclosure would prejudice safeguarding or other interests
- Only withhold information where legally justified

13.7 Children's SARs

For pupils:

- **Under 13:** Parents typically make requests on their behalf
- **13 and over:** We assess the child's competence to make their own request. If competent, parental consent is not required

14. Privacy Notices

Landon School provides clear, accessible privacy notices to explain how we use personal data. We have separate privacy notices for:

- Pupils and parents/carers
- Staff (teaching and non-teaching)
- Governors
- Visitors and volunteers
- Website users

14.1 Content of Privacy Notices

Our privacy notices include:

- What data we collect and why
- Our lawful basis for processing
- Who we share data with
- How long we keep data
- Individual rights
- How to contact us and the ICO

14.2 Accessibility

Privacy notices are:

- Published on our website
- Provided to parents at admission
- Given to staff at recruitment
- Written in clear, plain language
- Available in alternative formats on request

14.3 Review

Privacy notices are reviewed annually and updated whenever there are significant changes to data processing.

15. Data Protection Impact Assessments (DPIAs)

15.1 When DPIAs Are Required

A DPIA must be conducted before starting any processing that is likely to result in a high risk to individuals' rights and freedoms. This includes:

- Using new technologies or systems that process personal data
- Large-scale processing of special category data
- Systematic monitoring (e.g., new CCTV systems)
- Automated decision-making with significant effects
- Processing vulnerable individuals' data in new ways

15.2 DPIA Process

DPIAs involve:

1. Describing the processing and its purposes
2. Assessing necessity and proportionality
3. Identifying and assessing risks to individuals
4. Identifying measures to mitigate risks
5. Consulting the DPO
6. Documenting outcomes
7. Reviewing and updating as needed

15.3 Consulting the ICO

If a DPIA identifies a high risk that cannot be mitigated, we must consult the Information Commissioner's Office before proceeding with the processing.

16. Data Breaches

16.1 What is a Data Breach?

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

Examples include:

- Sending an email to the wrong recipient
- Loss or theft of a device containing personal data
- Unauthorized access to systems
- Ransomware attack encrypting data
- Accidental disclosure of data on social media
- Loss of paper records

16.2 Reporting Breaches

Staff must report any suspected or actual data breach immediately to:

Headteacher: Mr Jody Tranter

DPO: Jark Sekhon, School Business Manager

How to report: Email, phone, or in person - do not delay!

16.3 Responding to Breaches

Upon receiving a breach report, we will:

1. **Contain the breach:** Take immediate action to stop further data loss (e.g., revoke access, retrieve emails)
2. **Assess the breach:** Determine scope, severity, and individuals affected
3. **Notify if required:**
    a. Report to ICO within 72 hours if breach poses risk to individuals
    b. Notify affected individuals without undue delay if high risk to their rights
4. **Document:** Record details of the breach, actions taken, and decisions made
5. **Review and learn:** Identify lessons learned and implement preventive measures

16.4 ICO Notification

We must notify the ICO within 72 hours if the breach is likely to result in a risk to individuals' rights and freedoms, unless the breach is unlikely to pose such risk.

16.5 Individual Notification

We must notify affected individuals without undue delay if the breach is likely to result in a high risk to their rights and freedoms.

16.6 Breach Log

We maintain a log of all data breaches (regardless of whether ICO notification was required) including:

- Date and time of breach
- Description of breach
- Data affected
- Number of individuals affected
- Actions taken
- Whether ICO/individuals were notified

17. Training and Awareness

17.1 Mandatory Training

All staff members must complete:

- **Induction training:** Data protection basics within first week of employment
- **Annual refresher training:** Updated training each academic year
- **Role-specific training:** Additional training for staff with greater data responsibilities

17.2 Training Content

Training covers:

- UK GDPR principles and individual rights
- Lawful bases for processing
- Special category data handling
- Data security best practices
- Recognising and reporting data breaches
- Password and email security
- Subject access request procedures
- Confidentiality and information sharing

17.3 Training Records

We maintain records of all data protection training completed by staff members.

17.4 Ongoing Awareness

We promote data protection awareness through:

- Regular staff bulletins and reminders
- Posters and visual aids in staff areas
- Updates on changes to legislation or procedures
- Discussion at staff meetings

18. Appendices

Appendix A: Key Contacts

Role	Name	Contact Details
Headteacher	Mr Jody Tranter	Email: ofice@landonschool.co.uk Phone: 0208 153 0201

Proprietor	Mr Andy Thompson	Email: proprietor@landonschool.co.uk
Data Protection Officer	Jarka Sekhon	Email: dpo@landonschool.co.uk Phone: 0208 153 0201
Information Commissioner's Office	ICO	Website: www.ico.org.uk Phone: 0303 123 1113 Report a concern: ico.org.uk/concerns

Appendix B: Appropriate Policy Document (Special Category Data)

See separate document: "Landon School - Appropriate Policy Document for Special Category Data"

Appendix C: Full Data Retention Schedule

See separate document: "Landon School - Data Retention Schedule"

Appendix D: Data Processing Agreement Template

See separate document: "Landon School - Data Processing Agreement Template"

Appendix E: Subject Access Request Form

Available on school website and from school office

Appendix F: Data Breach Report Form

Available on staff intranet and from school office

This policy is available on our website and in alternative formats upon request.
Landon School is committed to safeguarding and promoting the welfare of children.