

Data Protection Policy

Reviewed and approved:	Compliance Officer
	May 2026
Next review due:	May 2027



Definitions and Applicability

This Policy should be read in conjunction with the following:

- Dragon School Privacy Notice
- Dragon School Privacy Notice for Children
- Dragon School Data Retention Policy
- [Dragon School Safeguarding Policy](#)
- Dragon School ICT Acceptable Use Policy
- Dragon School Use of School IT Devices Policy
- Dragon School ICT Acceptable Use Policy (Pupils)
- Security Policy (covering CCTV)
- [Data protection in schools - Guidance - GOV.UK](#)

BARDWELL ROAD
OXFORD OX2 6SS
Tel: +44 (0)1865 315400
www.dragonschool.org

This Policy applies to:

- The Prep School, the Pre-Prep School and EYFS;
- Current pupils, their parents and carers, colleagues, contractors, volunteers, governors, and anyone else working on behalf of the School;
- Former pupils, their parents and carers, colleagues, contractors, volunteers, governors, and anyone else who has worked on behalf of the School; and
- Prospective pupils, their parents and carers, colleagues, contractors, volunteers, governors, and anyone else who intends to work on behalf of the School.

In this Policy:

- “Data Controller” means the person or legal entity which determines the purpose for which and the means by which personal data is processed. The Dragon School Trust Limited is the School’s ultimate Data Controller.
- “Data Processor” means a person or legal entity which processes personal data on behalf of a data controller. Many individuals act as Data Processors within the School.
- “Data Protection law” includes but is not limited to the UK General Data Protection Regulation and the UK Data Protection Act 2018.
- “Data Subject” means the individual whose personal data is processed.
- “Personal Data” means information which can be used to identify a living person.
- “Processing” means an operation or set of operations applied to personal data. This may include but is not limited to collection, organisation, storage, use, disclosure, dissemination, and destruction. At the School, processing should be interpreted as any action performed on personal data.
- “School” means the Dragon School, Oxford.

Policy Aims and Principles

The purpose of this Policy is to provide a framework for ensuring that the School meets its obligations under Data Protection law, guided by the seven principles of data protection which require:

Principle	Explanation
Lawfulness, fairness and transparency	Data shall be processed lawfully, fairly and in a transparent manner
Purpose limitation	Data shall be collected for specified, explicit and legitimate purposes
Data minimisation	Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	Data shall be accurate and kept up to date
Storage limitation	Data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
Integrity and confidentiality (security)	Data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
Accountability	The School must be able to evidence its compliance with the above six principles and make sure that we do not put individuals at risk because of processing their personal data.

As part of Dragon School's commitment to safeguarding, the School has a particular duty to protect the personal data of its pupils.

LEGAL BASIS FOR PROCESSING

The School processes personal data under the following lawful bases:

Basis	Example (non-exhaustive)
Consent	Sharing certain individual achievements in publications
Contractual necessity	Processing parent contracts
Legal obligation	Sharing safeguarding information with local authorities or third party agencies
Vital interests	Emergency healthcare
Public interest	Provision of census information to the Department for Education
Legitimate interests*	Day to day processing required in order to provide education

*As a school, the 'north star' of our data collection and processing is in order to provide our pupils with their education. There are five key strands to this:

1. Supporting pupil learning
2. Monitoring and reporting on pupil progress
3. Providing appropriate pastoral key
4. Ensuring the safety and welfare of our pupils and colleagues
5. Managing our school's operations.

DATA SHARING AND SECURITY

It will be necessary and appropriate at time for the School to share personal information with third parties including

- Local authorities
- The Department for Education and other regulatory bodies
- The NHS and other health services

- Education software providers

We implement appropriate technical and organisational measures in order to

- Prevent unauthorised access, alteration, disclosure and destruction of personal information; and
- Ensure data accuracy and availability.

Please contact the Director of IT for further information on the details of these measures.

The School recognises that some members of its community may have heightened privacy and security requirements. The School expects all staff and members of the community to treat personal information confidentially and in accordance with the terms of this policy, as well as the School's policies on Safeguarding and ICT Acceptable Use as set out above.

Personal data is retained only for as long as necessary. Please refer to our Data Retention Schedule for further details.

RIGHTS OF THE DATA SUBJECT

The data subject also has rights under the Data Protection laws. These are:

Right	How this is achieved
The right to be informed	The School's Privacy Notices (including in an accessible format for children) are available on the School website
The right of access	The School will respond to subject access requests unless they are found to be manifestly unfounded or excessive.
The right to rectification	The School will take steps to validate information provided by data subjects and amend these details where necessary.
The right to erasure	The School will make reasonable efforts to comply with requests for erasure provided that it is not required to retain the information for one of the following reasons: • Right of freedom of expression and information • Compliance with a legal obligation • To protect archiving purposes in the public interest • The personal data is relevant to a legal claim
The right to restrict processing	Requests should be directed to the Compliance Officer.
The right to data portability	Requests should be made to the appropriate colleague (e.g. Deputy Head Pastoral for Safeguarding information, Director of HR for HR-related information) and requests will be processed in conjunction with the Compliance Officer.
The right to object	Requests should be directed to the Compliance Officer.
The right to withdraw consent	Requests should be directed to the Compliance Officer.
Rights in relation to automated decision making and profiling.	Requests should be directed to the Compliance Officer.

DATA BREACHES

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

Colleagues must inform the Compliance Officer as soon as they become aware that a personal data breach has taken place. Notifications should include the following:

- A description of the breach
- The type and volume of data involved
- The individuals affected
- Any actions already taken

The Compliance Officer will then

- Assess the details of the breach
- Contain the breach and mitigate any further risk
- Determine whether the breach is likely to result in a risk to the rights and freedoms of individuals.
 - If it is, the Compliance Officer will notify the Information Commissioner's Office within 72 hours.
 - In all circumstances, affected individuals will be informed without undue delay, including details of the breach and recommended actions.
- Practical steps will be taken in order to continuously improve data security and data protection awareness when data breaches occur within the School.

All breaches, regardless of their severity, will be documented in the school's Data Breach Log.

Regular training will be provided to colleagues to prevent data breaches and ensure prompt reporting, and technical and organisational measures will be reviewed regularly to enhance data security.