



Blue Sky Learning

G.D.P.R. and Data Protection Policy

Approved by: Kirsty Burridge
Date Approved: June 2026
Review Date: August 2027

1. Policy Statement

Blue Sky Learning is committed to protecting the privacy, confidentiality and security of personal information.

We process personal data in accordance with the Data Protection Act 2018, UK GDPR and other relevant legislation. We recognise our responsibility to ensure that personal information relating to pupils, families, staff, volunteers, contractors and visitors is handled lawfully, fairly and securely.

2. Legislation and Guidance

This policy is informed by:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Keeping Children Safe in Education (KCSIE)

This policy should be read alongside:

- Privacy Notices
- Records Retention Schedule
- Safeguarding and Child Protection Policy
- Email, Internet and Digital Communications Policy
- AI Use Policy

3. Data Protection Principles

Blue Sky Learning will ensure that personal data is:

- Processed lawfully, fairly and transparently.
- Collected for specified and legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and kept up to date.
- Retained only for as long as necessary.
- Kept secure and protected from unauthorised access, loss or misuse.

4. Roles and Responsibilities

Headteacher

The Headteacher is responsible for:

- Ensuring compliance with data protection legislation.
- Promoting good information governance practices.
- Managing data protection concerns and breaches.
- Supporting staff training and awareness.

Staff

All staff are responsible for:

- Handling personal information securely.
- Accessing information only where required for their role.
- Following provision policies and procedures.
- Reporting data breaches or concerns immediately.
- Protecting passwords, devices and confidential information.

Failure to comply with this policy may result in disciplinary action.

5. Processing Personal Information

Blue Sky Learning processes personal information for purposes including:

- Education and learning support.
- Safeguarding and welfare.
- SEND provision.
- Employment and human resources.
- Health and safety.
- Legal and regulatory requirements.

Information will only be collected, used and shared where there is a lawful basis to do so.

6. Information Security

Blue Sky Learning will take appropriate technical and organisational measures to protect personal information.

This includes:

- Secure storage of paper and electronic records.
- Password protection and access controls.
- Secure disposal of confidential information.
- Use of approved systems and software.
- Cyber security measures to reduce the risk of unauthorised access.

Staff must:

- Keep passwords secure.
- Lock devices when unattended.
- Be alert to phishing emails and cyber threats.
- Report lost devices or information immediately.
- Not store confidential information on personal devices unless authorised.

7. Data Sharing

Personal information will only be shared where:

- There is a lawful basis for doing so.
- It is necessary to support education, safeguarding or welfare.

- It is required by law.
- Appropriate safeguards are in place.

Information sharing decisions will always consider the safety, rights and privacy of individuals.

Safeguarding concerns may require information to be shared without consent where this is necessary to protect a child or vulnerable person.

8. Individual Rights

Individuals have rights under data protection legislation, including the right to:

- Access their personal information.
- Request correction of inaccurate information.
- Request restriction of processing where appropriate.
- Object to processing in certain circumstances.
- Make a complaint to the Information Commissioner's Office (ICO).

Requests relating to personal information will be managed in accordance with statutory requirements.

9. Data Breaches

All actual or suspected data breaches must be reported immediately to the Headteacher.

Breaches will be investigated promptly and, where required, reported to the Information Commissioner's Office (ICO) within statutory timescales.

Appropriate action will be taken to minimise any potential impact.

10. Training

All staff will receive appropriate training and guidance regarding:

- Data protection responsibilities.
- Information security.
- Cyber security awareness.
- Safe use of digital systems.
- Confidentiality and safeguarding.

Training will be refreshed regularly.

11. Monitoring and Review

This policy will be reviewed annually or sooner if legislation, guidance or operational requirements change.