



1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents/carers, governors, visitors and other individuals 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, regardless of whether it is held in paper or electronic format.

2. Legislation and Guidance

This policy meets the requirements of the UK GDPR and the Data Protection Act 2018. It is based on guidance published by the Information Commissioner's Office (ICO).

It also complies with the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Information relating to an identified or identifiable individual
Special category data	Sensitive personal data such as health, ethnicity or safeguarding information
Processing	Any action performed on personal data (collection, storage, use, sharing or deletion)
Data subject	The individual the data relates to
Data controller	The organisation that decides how and why personal data is processed
Data processor	A third party processing data on behalf of the controller
Personal data breach	A security incident leading to accidental or unlawful loss, access or disclosure of personal data

4. The Data Controller

Barnet Early Years Alliance (BEYA) processes personal data relating to pupils, parents/carers, staff, governors and visitors and is therefore a data controller.

BEYA is registered with the Information Commissioner's Office (ICO) and pays the data protection fee as required by law.

5. Roles and Responsibilities

Governing Board

Responsible for ensuring compliance with data protection law.

Data Protection Officer (DPO)

Responsible for overseeing data protection compliance and acting as the contact point for individuals and the ICO.

DPO Contact:

Satswana

Email: admin@satswana.com

Address: Suite G12 Ferneberga House, Alexandra Road, Farnborough, Hampshire, GU14 6DQ

Headteacher

Kelly Brooker

Responsible for day-to-day compliance.

All Staff

Responsible for:

- Handling personal data securely and lawfully
- Reporting breaches immediately
- Only accessing data required for their role
- Following all school policies

6. Data Protection Principles

Personal data must be:

- Processed lawfully, fairly and transparently
- Collected for specified and legitimate purposes
- Adequate, relevant and limited to necessity
- Accurate and kept up to date
- Kept only as long as necessary
- Processed securely

7. Collecting Personal Data

We only process personal data where a lawful basis applies:

- Contract
- Legal obligation
- Public task
- Vital interests
- Legitimate interests
- Consent (where appropriate)

Data will only be used for the purpose it was collected for unless otherwise stated.

8. Sharing Personal Data

We may share personal data with:

- Local authorities
- The Department for Education
- Ofsted
- Health authorities
- Police, courts and tribunals
- Safeguarding partners
- Service providers and contractors
- Professional advisers
- Government departments and agencies
- Emergency services
- Other organisations where required by law

Appropriate data sharing agreements are used where required.

9. CCTV

Barnet Early Years Alliance (BEYA) operates closed-circuit television (CCTV) systems across its nursery schools and children's centres for safeguarding, security and operational purposes.

CCTV is used for:

- Safeguarding children, staff, parents/carers and visitors
- Supporting investigation of incidents, accidents and safeguarding concerns
- Preventing and detecting crime, vandalism and anti-social behaviour
- Protecting school property and premises
- Supporting safety and security of buildings and grounds

Lawful Basis

Processing of CCTV footage is carried out under:

- UK GDPR Article 6(1)(e) – Public Task
- UK GDPR Article 6(1)(f) – Legitimate Interests

Access and Disclosure

Access to CCTV footage is strictly limited to authorised personnel.

CCTV footage may be shared with:

- Police
- Local authority services
- Children's social care
- Safeguarding partners
- Legal advisers
- Insurance providers
- Regulatory bodies

where there is a lawful basis to do so.

Retention

CCTV footage is normally retained for up to **30 days**, after which it is automatically overwritten.

Footage may be retained longer where required for:

- Safeguarding investigations
- Incident or accident investigations
- Disciplinary procedures
- Insurance claims
- Legal proceedings
- Criminal investigations

CCTV Requests

Requests to access CCTV footage will be considered in accordance with UK GDPR and the Data Protection Act 2018.

There is no automatic right to view CCTV footage. Each request is assessed individually, taking into account the rights of other individuals who may appear in the footage.

Further details are set out in the BEYA CCTV Policy.

10. Subject Access Requests (SARs)

Individuals have the right to request access to personal data held about them.

Requests must include:

- Name
- Contact details
- Description of the information requested

Requests must be sent to the DPO:

admin@satswana.com

We respond within one calendar month (extendable if complex).

11. Parental Requests for Educational Records

Parents/carers may request access to their child's educational record, which will be provided within 15 school days.

12. Photographs and Videos

Consent is obtained from parents/carers before photographs or videos are used for:

- School displays
- Publications
- Website or social media
- External media

Consent can be withdrawn at any time.

13. Data Protection by Design

We ensure data protection is embedded through:

- Staff training
- Data minimisation

- Risk assessments
- Secure systems and controls
- Regular policy review
- Record keeping of processing activities

14. Data Security

We protect personal data through:

- Secure storage of paper records
- Password-protected systems
- Encryption of devices
- Controlled access based on job roles
- Secure transfer of data

15. Disposal of Records

Personal data is securely destroyed when no longer required using shredding or permanent deletion methods.

16. Personal Data Breaches

The school takes data security seriously and has procedures in place to manage any breach.

In the event of a breach, the DPO will:

- Investigate and contain the breach
- Assess risk to individuals
- Report to the ICO within 72 hours where required
- Notify affected individuals where necessary
- Record all incidents

17. Training

All staff receive data protection training during induction and regularly thereafter.

18. Monitoring and Review

The Data Protection Officer monitors compliance with this policy.

This policy is reviewed annually or sooner if required.