CREATIVE, DIGITAL & PERFORMING ARTS ACADEMY

Data Protection Policy

Author	Mark Allen / Chris Mitchell
Approved by	Alistair Chattaway
Trustees' approval date	
Release date	September 2026
Review date	September 2028
Description of changes	• Updated the legislative framework to the Data (Use and Access) Act 2025 and updated references to KCSIE 2026 and current DfE standards. • Added the statutory data protection complaints process and response requirements. • Updated subject access procedures, including verbal requests, reasonable and proportionate searches, clarification and children's competence. • Updated safeguarding file transfers and filtering and monitoring review and record-keeping requirements. • Strengthened multi-factor authentication and cyber security requirements. • Updated safeguards for automated decision-making and children's biometric data.

Aims

BOA Academy Trust aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors, contractors, and other individuals is **collected, stored, and processed** in accordance with:

- UK General Data Protection Regulation (**UK GDPR**)
- Data Protection Act 2018 (**DPA 2018**)
- Data (Use and Access) Act **2025**
- Keeping Children Safe in Education (KCSIE) 2026
- Relevant statutory and DfE guidance

We are committed to protecting individuals' rights, ensuring transparency, and supporting safeguarding duties under **KCSIE 2026**.

Scope

This policy applies to:

- All personal data processed by BOA
- Staff, trustees, volunteers, contractors, and third parties
- Data stored electronically, on paper, or by other means

Legislation and guidance

This policy reflects:

- UK GDPR and DPA 2018 requirements
- **Data (Use and Access) Act 2025** requirements, including complaints handling, subject access clarification, reasonable and proportionate searches, and automated decision-making safeguards
- ICO guidance on subject access, surveillance, children's data, and international transfers
- DfE statutory guidance:
    - **KCSIE 2026**
    - Information Sharing (2024)
    - Cyber Security Core Standard (current version)
    - Filtering and Monitoring Core Standard (current version)

It cross-references the following BOA policies:

- **Safeguarding & Child Protection Policy**
- **E-Safety & Online Safety Policy**
- **Acceptable Use Policy**
- **Privacy Notices**

Definitions

Term	Definition
Personal data	Any information identifying an individual
Special category data	Sensitive data requiring extra protection (e.g. health, ethnicity, biometrics, beliefs)
Processing	Any operation on data (collection, storage, sharing, erasure)
Data controller	BOA Academy Trust
Data processor	Third party processing data on BOA's behalf
Personal data breach	A security incident leading to loss, disclosure, or unauthorised access

Roles and responsibilities

Trustees

- Ensure BOA complies with all data protection obligations

Principal

- Acts as BOA's data controller representative

Data Protection Officer (DPO)

- Oversees compliance
- Advises on data protection matters
- Liaises with the ICO
- Monitors DPIAs and breach responses
- Contact: **wayne.adams@boa-group.co.uk**

All Staff

- Follow this policy and handle personal data securely
- Report any suspected data breaches immediately

Data protection principles

BOA complies with the six UK GDPR principles. Personal data must be:

1. Processed **lawfully, fairly, and transparently**
2. Collected for **specified, explicit, and legitimate purposes**
3. **Adequate, relevant, and limited** to what's necessary
4. **Accurate** and kept up to date
5. Retained **no longer than necessary**
6. Processed **securely** to protect confidentiality and integrity

Collecting and Using Personal Data

We will only process personal data where we have a lawful basis under UK GDPR and the DPA 2018, as amended by the Data (Use and Access) Act 2025.

Lawful Bases

We rely on the following lawful bases:

- **Public task** – delivering education, safeguarding, and statutory functions
- **Legal obligation** – complying with laws (e.g. exam regulations, attendance reporting)
- **Vital interests** – protecting life or wellbeing
- **Consent** – freely given (e.g. media use, optional surveys)
- **Legitimate interests** – carefully balanced against individual rights

Special Category Data

Special category data (e.g. health, ethnicity, biometrics, safeguarding) is processed under **Schedule 1, DPA 2018**, particularly for safeguarding and equalities monitoring.

Privacy Notices

Individuals are provided with privacy notices explaining:

- Why data is collected
- How it is used
- Who it is shared with
- Retention periods

Sharing personal data

We will not normally share personal data, but may do so:

- To fulfil safeguarding obligations under **KCSIE 2026**
- With statutory agencies (e.g. DfE, Ofsted, LA, exam boards)
- With law enforcement where legally required
- With trusted third-party processors (e.g. IT providers, caterers)

Safeguarding records will be transferred securely and separately from the main pupil file as soon as possible, and within 5 days for an in-year transfer or within the first 5 days of a new term. The exporting setting will obtain confirmation of receipt and include a clear, structured summary of current concerns, relevant context and ongoing support needs, in line with **KCSIE 2026**.

We will ensure all processors:

- Have data protection agreements in place
- Provide sufficient guarantees of compliance
- Only receive the minimum necessary data

Subject access and individual rights

Under UK GDPR, individuals have the right to:

- Access their personal data (subject access request)
- Rectify inaccurate data
- Request erasure where lawful
- Restrict or object to processing
- Request portability of their data
- Receive appropriate safeguards where solely automated processing produces a legal or similarly significant decision, including information about the decision and the ability to make representations, obtain human intervention and contest it

Subject access requests may be made verbally or in writing, including by email or social media, and may be made to any part of BOA. Staff must record and promptly refer requests to the DPO. BOA will respond without undue delay and within one month of receipt, or of receiving information reasonably required to confirm identity. Where necessary, the period may be extended by up to two further months. BOA will carry out a reasonable and proportionate search. Where clarification is reasonably required, the response period may be paused until clarification is received.

Children's rights belong to the child. In England there is no fixed age at which a child is presumed competent to exercise them. Competence will be assessed case by case, considering the child's maturity and understanding, the nature of the information, the consequences of the request and the child's best interests. Age 12 may be a useful guide, but it is not a presumption.

Data protection complaints

BOA provides an accessible way for individuals to complain about how their personal data is used. Complaints may be made verbally or in writing, including by email, to the DPO.

- Receipt of a complaint will be acknowledged within 30 days.

- BOA will make appropriate enquiries and take appropriate steps to respond without undue delay.
- The complainant will be kept informed of progress and told the outcome without undue delay.
- Complaints and their outcomes will be documented.
- The outcome will explain the right to complain to the Information Commissioner's Office if the complainant remains dissatisfied.

Data Protection by Design and DPIAs

We integrate data protection into all our systems and projects.

DPIAs (Data Protection Impact Assessments) will be conducted where processing is likely to result in high risk, including:

- Biometrics (e.g. cashless catering, access systems)
- CCTV and surveillance systems
- AI-powered educational tools
- Cloud-based platforms and third-party apps

The **DPO** must be consulted on all DPIAs.

Biometric data

Where BOA uses an automated biometric recognition system involving a person under 18, it will comply with the Protection of Freedoms Act 2012 and current DfE guidance. This includes notifying parents, obtaining the required written parental consent, respecting a student's objection and providing a reasonable alternative.

CCTV

- CCTV is used for **security and safeguarding** purposes
- Operated in compliance with the **ICO Code of Practice** and **Surveillance Camera Code**
- Signage clearly indicates where cameras are in use
- Images are retained securely and for no longer than necessary
- Any enquiries about the CCTV system should be directed to john.wilson@boa-academy.co.uk (Head of Estates)

Photographs and videos

- **Consent** will be obtained before photographs or videos are taken for non-statutory purposes
- Consent can be withdrawn at any time
- Pupils' images will not be published with identifying information without consent
- Uses may include newsletters, school website, social media, or promotional material
- See our child protection and safeguarding policy for more information on our use of photographs and videos.

Online Safety, Filtering, and AI

We comply with **KCSIE 2026** and DfE filtering/monitoring standards:

- The effectiveness of filtering and monitoring is reviewed at least once each academic year by the responsible member of SLT with the DSL, IT support and responsible governor; results and actions are recorded
- Safeguarding and IT checks cover school-managed internet-connected devices, services, user groups and locations; each check is logged with the date, person, scope and resulting action
- Additional reviews are undertaken when risks, working practices, new technology, major updates or configurations change; safeguarding staff are trained to interpret monitoring data

Generative AI tools are subject to additional controls:

- Use must be supervised and risk-assessed
- **DPIAs** are required for AI-based educational tools
- Students will not be permitted to use AI services without age-appropriate safeguards
- Staff must follow BOA's **E-Safety & Online Safety Policy** when using AI tools

Data Security

We take appropriate technical and organisational measures to protect personal data against unauthorised or unlawful access, alteration, processing, or disclosure, and against accidental loss or destruction.

Measures include:

- Encryption of portable devices and secure storage of records
- **Multi-factor authentication (MFA)** must be enabled for all staff accounts accessing cloud services or remotely accessing on-site systems, and for all IT administrative accounts. Where MFA is unavailable, stronger alternative password controls will be used
- Role-based access controls
- Secure transfer protocols for sharing personal data
- Staff training on secure data handling
- Regular review of security in line with the current **DfE Cyber Security Core Standard**

Retention and Disposal of Records

- Personal data will be retained only for as long as necessary, in accordance with the **IRMS Records Management Toolkit for Schools**
- When no longer needed, data will be disposed of securely:
    - Paper records will be shredded or incinerated
    - Electronic files will be securely wiped or overwritten

- Third-party providers will supply destruction certificates where applicable

Personal Data Breaches

We make every effort to avoid personal data breaches, but where they occur:

1. **Immediate Reporting**
   - All staff must report any actual or suspected breach to the **DPO** immediately.
2. **Investigation and Containment**
   - The DPO will investigate, assess risk, and take necessary steps to mitigate damage.
3. **ICO Notification**
   - Where a breach is likely to result in a risk to individuals' rights and freedoms, the **ICO will be notified within 72 hours**.
4. **Informing Affected Individuals**
   - Where the risk is high, we will inform affected individuals promptly.
5. **Recording Breaches**
   - All breaches are logged, regardless of severity, including actions taken and lessons learned.

Staff Training

All staff, volunteers, trustees, and contractors receive:

- **Induction training** on data protection and safeguarding
- **Annual refresher training** on data security, online safety, and AI use
- Role-specific training where appropriate (e.g. safeguarding, IT administration)
- Awareness sessions on **KCSIE 2026** changes and expectations

Monitoring and Review

- This policy is reviewed **every two years** or sooner if significant legal or regulatory changes occur
- The **DPO** monitors compliance, audits processes, and reports annually to the Trustees
- Related policies (e.g. **Safeguarding & Child Protection**, **E-Safety & Online Safety**, **Acceptable Use**) are reviewed alongside this document for consistency

Links with other policies

This data protection policy is linked to our:

- Acceptable Use Policy
- Child Protection and safeguarding Policy
- E-Safety Policy

Appendix 1: Personal data breach procedure

This procedure is based on ICO guidance:

1. **Identification**
    - Any member of staff discovering a breach must report it immediately to the **DPO**.
2. **Containment**
    - Steps will be taken to prevent further data loss or exposure.
3. **Risk Assessment**
    - The DPO will assess potential harm, considering likelihood and severity.
4. **ICO Notification**
    - If required, the breach will be reported via the ICO's portal within **72 hours**.
5. **Communication with Data Subjects**
    - Where high risk exists, individuals affected will be contacted directly.
6. **Review and Prevention**
    - Following any breach, BOA will conduct a review and update processes or training where necessary.