CREATIVE, DIGITAL & PERFORMING ARTS ACADEMY

# Data Protection Policy

| | |
|---|---|
| Author | Mark Allen / Chris Mitchell |
| Approved by | Alistair Chattaway |
| Trustees approval | |
| Release date | September 2025 |
| Review date | September 2027 |
| Description of changes | • Added compliance with the Data Protection and Digital Information Act 2025 (DPDI Act).<br>• Integrated KCSIE 2025 requirements (safeguarding, filtering/monitoring, AI, file transfer timelines).<br>• Introduced DPIAs for AI, biometrics, CCTV, and high-risk platforms.<br>• Strengthened data sharing rules with explicit safeguarding exemptions.<br>• Enhanced online safety, filtering, monitoring, and AI usage controls.<br>• Aligned retention schedules with IRMS Toolkit and updated disposal practices.<br>• Expanded breach response procedures (ICO 72-hour rule, high-risk notifications).<br>• Improved training requirements, including annual refreshers and AI awareness. |

CREATIVE, DIGITAL & PERFORMING ARTS ACADEMY

## 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 Protection and Digital Information Act **2025**
- **Keeping Children Safe in Education (KCSIE) 2025**
- Relevant statutory and DfE guidance

We are committed to protecting individuals' rights, ensuring transparency, and supporting safeguarding duties under **KCSIE 2025**.

## 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
- **DPDI Act 2025** changes (e.g. DSAR "stop-the-clock" and updated lawful bases)
- ICO guidance on subject access, surveillance, children's data, and international transfers
- DfE statutory guidance:
    - **KCSIE 2025**
    - Information Sharing (2024)
    - Cyber Security Standards (2024)
    - Filtering & Monitoring Standards (2023)

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.

**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 2025**
- 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 to a new school or provider within **5 school days**, in line with **KCSIE 2025**.

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
- Object to automated decision-making

**Requests** must be made in writing (including email) and will be processed within **one month** (or extended to 3 months if complex). Identification may be required.

Children aged **12 and above** are usually considered competent to exercise their own rights, unless assessed otherwise.

## 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.

## 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 2025** and DfE filtering/monitoring standards:

- Filtering and monitoring systems are in place and reviewed annually
- Clear roles exist for oversight and escalation of concerns
- 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
- Strong passwords and **multi-factor authentication (MFA)** where possible
- Role-based access controls
- Secure transfer protocols for sharing personal data
- Staff training on secure data handling
- Annual review of security in line with **DfE Cyber Security Standards**

## 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 2025** 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 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.