



Data Protection Policy

XYZ Music Academy Ltd

Signed: Duncan Lee, Director

Date: 24.12.2025

Review Date: To be reviewed annually or following changes in legislation

Data Protection Officer (DPO): Duncan Lee

Contact: 01296 534032 | duncan@xyzmusicacademy.com

1. Introduction

XYZ Music Academy Ltd (“the Academy”) collects, processes, and stores personal data in order to deliver high-quality music education and related services. We are committed to protecting the privacy and rights of all individuals whose data we handle, with particular care given to children and young people.

This policy sets out how personal data is handled lawfully, fairly, and securely, whether stored electronically, on paper, or by other means. It applies to all staff, tutors, contractors, and third parties working on behalf of XYZ Music Academy Ltd.

The Academy complies with all relevant data protection legislation, including:

- UK General Data Protection Regulation (UK GDPR)
 - Data Protection Act 2018
 - Any other applicable data protection or privacy laws
-

2. Scope

This policy applies to all personal data processed by XYZ Music Academy Ltd, including data relating to:

- Children and young people
- Parents and guardians
- Employees, tutors, and contractors
- Suppliers and service providers

It covers all data processing activities, including collection, storage, use, sharing, and disposal of personal data in both digital and physical formats.

3. Definitions

Personal Data

Any information relating to an identifiable individual, directly or indirectly. This includes names, contact details, dates of birth, payment information, and opinions relating to an individual.

Data Subject

The individual to whom the personal data relates.

Special Category Data

Personal data revealing health information, ethnicity, religion, biometric data, or other sensitive characteristics.

Criminal Offence Data

Data relating to criminal convictions or allegations.

Data Processing

Any action performed on personal data, including collection, storage, use, disclosure, or deletion.

Data Controller

XYZ Music Academy Ltd, which determines how and why personal data is processed.

Data Breach

A security incident resulting in the loss, unauthorised access to, or disclosure of personal data.

4. Data Protection Principles

XYZ Music Academy Ltd processes personal data in accordance with the UK GDPR principles:

- a) Processed lawfully, fairly, and transparently
 - b) Collected for specified, explicit, and legitimate purposes
 - c) Adequate, relevant, and limited to what is necessary
 - d) Accurate and kept up to date
 - e) Retained only for as long as necessary
 - f) Processed securely using appropriate technical and organisational measures
 - g) Transferred internationally only in compliance with GDPR requirements
-

5. Roles and Responsibilities

The **Director and Data Protection Officer (DPO)** is responsible for:

- Overseeing compliance with this policy
- Handling data protection queries and complaints
- Managing data breaches and Subject Access Requests
- Reviewing and auditing data protection practices

The **General Manager** supports auditing and compliance monitoring.

All staff, tutors, and contractors are responsible for:

- Following this policy
 - Protecting personal data they handle
 - Reporting concerns or data breaches immediately
-

6. Collection and Use of Personal Data

Consent and Privacy Notices

- Consent is obtained from parents or guardians before collecting children's data
- Clear privacy notices explain why data is collected, how it is used, and how long it is kept
- Privacy notices are written in clear, accessible language

Data Minimisation and Purpose Limitation

- Only data necessary to deliver music tuition, manage safeguarding, or meet legal obligations is collected
- Personal data is used only for the purpose it was collected unless further consent or legal authority applies

Data Security Safeguards

- Secure systems, password protection, and restricted access are used
 - Physical records are stored securely
 - Access is limited to authorised personnel on a need-to-know basis
-

7. Data Breach Management

All data breaches must be reported immediately to the DPO.

Breach Response

The DPO will:

- Assess whether the breach is ongoing and take steps to contain it
- Investigate the cause and impact
- Determine whether the Information Commissioner's Office (ICO) must be notified within 72 hours
- Inform affected individuals where there is a high risk to their rights and freedoms
- Keep detailed records of the breach and actions taken

Breaches may include loss of devices, unauthorised access, cyber-attacks, or human error.

8. Data Retention and Disposal

Personal data is retained only for as long as necessary.

Employees and Tutors

- Data is securely destroyed when employment or engagement ends, unless legally required otherwise

Children and Parents

- **Active students:** Data retained for the duration of enrolment
- **Inactive students:** Data retained for up to one year after last engagement
- **Deletion requests:** Data will be erased promptly unless legal obligations apply

All data is securely deleted or destroyed when no longer required.

9. Data Subject Rights

Individuals have the right to:

- Access their personal data
- Correct inaccurate or incomplete data
- Withdraw consent (where applicable)
- Request erasure or restriction of processing
- Object to certain types of processing
- Be informed of data breaches affecting them
- Lodge a complaint with the ICO
- Request data portability in limited circumstances

Identity verification is required before rights are exercised.

10. Subject Access Requests (SARs)

Requests may be made in writing or verbally and must be forwarded immediately to the DPO.

- Requests will be acknowledged promptly
- Responses will be provided within one calendar month
- Additional identification or clarification may be requested

Requests Involving Children

- The right of access belongs to the child
- Children aged 12+ are presumed capable of making their own request
- Parental access may be restricted where disclosure could harm the child

All SARs are recorded and managed by the DPO.

11. Third-Party Data Sharing

Personal data is only shared with third parties:

- With explicit consent
- Where legally required
- To fulfil contractual or safeguarding obligations

All third-party providers must comply with data protection legislation and appropriate agreements will be in place.

12. Staff Training and Awareness

- All staff and tutors receive data protection training
 - Training is included in induction and refreshed regularly
 - Staff must report concerns or uncertainties to the DPO
-

13. Data Auditing and Monitoring

- Annual data protection audits are conducted
 - Continuous monitoring identifies potential risks
 - Audit reports document findings and actions taken
-

14. Policy Review

This policy is reviewed regularly to ensure ongoing compliance with legislation and best practice. Updates will be communicated to staff as required.

15. Statement of Commitment

XYZ Music Academy Ltd is fully committed to protecting the personal data of children, families, staff, and partners. By following this policy, we ensure that data is handled responsibly, securely, and in a way that supports a safe and professional music education environment.