



## Bromley Youth Music Trust

# Data Protection Policy

**April 2018 Edition**

**To be reviewed: April 2019**

Bromley Youth Music Trust is committed to safeguarding and promoting the welfare of children and young people and expects all staff to share this commitment.

Bromley Youth Music Trust is committed to valuing and celebrating diversity and promoting equality of opportunity for all its staff and students. We are working to create a learning and working environment which is free from prejudice, discrimination, intimidation and all forms of harassment including bullying. Respect for rights is at the heart of our planning, policies, practice and ethos and we expect all members of our community to model this in their behaviour and relationships

Supported using public funding by



**ARTS COUNCIL  
ENGLAND**



## **1 Introduction**

BYMT is required to process relevant personal data regarding members of staff, applicants and customers (parents, pupils, volunteers, alumni) as part of its operation and shall take all reasonable steps to do so in accordance with this Policy.

Personal Data is essentially personal information about an individual that is held electronically (on a computer) or held in a file.

Customer records include the following information:

- Personal information such as full name, address, date of birth, school, medical information
- Name of Parent/carer (where applicable) and contact information such as mobile telephone and email address
- Parent/carer bank details
- Invoicing and payment history
- Ensemble activity.

Staff records include:

- personal information; name, address, date of birth, DBS and other recruitment and or appointment information
- Bank details
- disciplinary/grievance/performance appraisal/capability and development records
- salary/overtime correspondence,
- any requests made to the Principal/ Deputy Principal for special leave and or flexible working

## **2 Aim of Policy**

BYMT recognises The EU General Data Protection Regulation (GDPR) that comes into force on 25 May 2018 and aims to ensure that Personal data shall be:

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary
4. Accurate and, where necessary, kept up to date
5. Retained only for as long as necessary
6. Processed in an appropriate manner to maintain security

Personal Data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data.

### **3 Data Retention**

The Trust is directly responsible under the Data Protection Act (DPA) for the collation, retention, storage and security of all information we produce and hold. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose. Information shall be securely deleted when it is no longer required. Data may be archived only if there is a possibility it may still be required.

### **4 Confidentiality**

BYMT will respect the confidentiality of information it processes. However, information will be disclosed on a need to know basis. For example, the relevant Office Staff or appropriate First Aider may disclose details of a pupil's allergy to bee stings so that other staff know how to respond, but personal contact details for parents will not be disclosed to other people unless BYMT has received their permission to do so.

**Care must be taken to ensure that only information that the individual is entitled to is released and that it does not include other sensitive information in error.**

### **5 Access**

Parents, pupils and staff are able to make a request under the DPA to find out if BYMT holds any Personal Data about them and what it is. This is called a *data subject access request*. Any data subject wishing to access their personal data should put their request in writing to the Head of Administration. BYMT will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event, within 40 days for access to records and 21 days to provide a reply to an access to information request.

### **6 Consent**

BYMT processes some personal data for direct marketing and fund-raising purposes, data subjects have the right to request an opt-out to these activities, which must be respected.

### **7 Security**

BYMT will take appropriate technical steps and implement organisational systems to ensure the security of personal data. All staff will be made aware of this policy.

BYMT and therefore all staff and pupils are required to respect the personal data and privacy of others and must ensure that appropriate protection and security measures are taken against unlawful or unauthorised processing of

personal data, and against the accidental loss of, or damage to all personal data.

Personal data must be stored in appropriate systems and be password protected if stored or sent electronically.

BYMT must ensure that data processed by external providers is compliant with this policy and the relevant legislation.

When data held in accordance with this policy is destroyed, it must be destroyed securely in accordance with best practice at the time of destruction.

## **8 Responsibility**

- The Deputy Principal (Head of Administration) will act as the appointed Data Protection Officer.
- The Senior Administrator will process data subject access requests for staff and customers.
- The Senior Administrator will process requests under the Freedom of Information Act. All requests must be approved by the Principal or, if the information requested is about the Principal, the Chair of Trustees.
- If you have a complaint about how information is processed, please contact the Deputy Principal (Head of Administration) in the first instance or see BYMT's published Complaints Procedure.

## **9 Further Information**

Staff should be aware of and compliant with BYMT:

1. Privacy policy
2. Card payments policy
3. ICT Acceptable use policy
4. Business Continuity plan
5. Staff Handbook