APPROPRIATE POLICY DOCUMENT

Responsible for Implementation: Data Protection Officer
Latest Review Date: October 2022
Next Review Date: October 2023
Authorised By: Director of Governance

Contents

About Us

Access to Music Limited ('The College') has subsidiary companies, trading names and trading partnerships through which it operates. The trading names and partnerships might have their own names or brands, but the legal entity for the purpose of this policy is Access to Music Limited. Trading subsidiaries, trading names and trading partnerships include Access Creative College ('ACC'), National College for Creative Industries ('NCCI') and Access Sport. The dBs Institute (DBS Music UK Holdings and its subsidiaries), whilst a separate legal entity, shares common Directorships with the College, however, responsibility for Data Protection related Policies within dBs falls to the DPO for Access to Music Limited

Introduction

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document to be in place when processing special category and criminal offence data under certain specified conditions as defined in Schedule 1.

Scope and Application

This Appropriate Policy Document will cover all processing of special category personal data carried out by The College for which all of the following conditions are met:

- We (data controller) are processing personal data which is the subject of Articles 9 or 10 of the UK GDPR.
- We (data controller) are processing this personal data in reliance of a condition listed in Parts 1, 2 or 3 of Schedule 1 of the DPA.
- The condition listed in Parts 1, 2 or 3 of Schedule 1 includes a requirement for the data controller to have an Appropriate Policy Document.

All staff, contractors and other authorised third parties must adhere to this policy.

Purpose

The purpose of this document is to explain what special category data is being processed by The College, the reasons for which we use this data, and the procedures for ensuring this processing complies with Article 5 of the UK GDPR. The document will also explain the policies relating to the retention and erasure of such data.

We process special category data in other instances where it is not a requirement to keep an appropriate policy document. Our processing of such data respects the rights and interests of the data subjects. We provide clear and transparent information about why we process personal data (including all special category data and criminal convictions/offences data we process) as well as our lawful basis for processing, in our Privacy Notice.

Relevant Categories of Data

Special category data, as defined by Article 9 of the UK GDPR, is personal data which reveals:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for the purpose of uniquely identifying a natural person
- Data concerning health
- Data concerning a natural person's sex life or sexual orientation

The College will not at any time process genetic data, biometric data for the purpose of uniquely identifying a natural person, or data concerning a natural person's sex life or sexual orientation.

We also process data as defined by Article 10 of the UK GDPR, relating to criminal convictions and offences or related security measures. Section 11(2) of the DPA 2018 states that criminal conviction data includes data which relates to the alleged commission of offences and related proceedings and sentencing.

UK GDPR Conditions for Processing

The conditions relied upon for processing the data sets outlined above are based on explicit consent and our employment law obligations. More information can be found in our General Privacy Policy; the Learner Privacy Notice, the Apprenticeships Privacy Notice and the Workforce Privacy Notice which are available to all learners, apprentices and staff.

Special category data as listed above is also processed for our Safeguarding obligations and more information can be found in the policies and notices above.

We process special category data for the following purposes permitted under Schedule 1 of the DPA 2018:

Part 1 - Conditions relating to Employment, Health and Research etc

1(1) - Employment, social security and social protection
The College may process data concerning racial or ethnic origin, religious or philosophical beliefs, trade union membership, health and criminal offence data for the purposes of performing its
obligations or rights as an employer, or for ensuring the social protection of individuals

2(2) - Health or social care purposes
The College may process data concerning health for the assessment of the working capacity of an employee.

Part 2 - Substantial Public Interest Conditions

8(1) - Equality of opportunity or treatment
The College may process data concerning racial or ethnic origin, religious or philosophical beliefs
and health for the purposes of monitoring equality of opportunity or treatment between groups of its employees and learners with a view to enabling such equality to be promoted or maintained.

10(1) - Preventing or detecting unlawful acts
The College may process data concerning health and criminal offences for the purposes of preventing and detecting crime, including where required the disclosure of such personal data to a competent authority.

14(1) - Preventing fraud
The College may disclose personal data in accordance with arrangements made by an anti-fraud organisation.

17(1) - Counselling etc…
The College may process data concerning health and criminal offences for the purposes of confidential counselling, advice or support or of another similar service provided confidentially.

18(1) - Safeguarding of children and of individuals at risk
The College may process data concerning health and criminal offences, religious or philosophical beliefs for the purposes of protecting an individual from neglect or physical, mental or emotional harm, or protecting the physical,

mental or emotional well-being of an individual, where said individual is aged under 18, or over 18 and at risk (as defined by the DPA 2018).

20 - Insurance
The College may process data concerning racial or ethnic origin, religious or philosophical beliefs, trade union membership, health and criminal offence data for insurance purposes.

Part 3 - Additional Conditions Relating to Criminal Convictions etc

29 - Consent
The College may process criminal offence data if the data subject has given consent to the processing

30 - Protecting individual's vital interests
The College may process criminal offence data where processing is necessary to protect the vital interests of an individual, and where the data subject is physically or legally incapable of giving consent.

The College processes criminal offence data for the purposes of employment, social security and social protection, and for the purposes of safeguarding children and individuals at risk.

Procedures for Ensuring Compliance with the Principles

As required by Data Protection Law, we ensure that all processing of personal data at the College is carried out in compliance with the data protection principles.

1. **Accountability principle**

The Company takes responsibility for complying with the UK GDPR and DPA 2018, at the highest level of management and throughout our organisation. We keep records of the steps we take to comply and review and update our accountability measures at appropriate intervals. The technical and organisational measures we have in place include:

- Maintaining records of our processing activities
- Adopting and implementing data protection policies
- Reviewing data protection, privacy and information security risks regularly
- Carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to the interests of individuals
- Implementing appropriate security measures and taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations
- Putting written contracts in place with organisations that process personal data on our behalf
- Appointing a Data Protection Officer

2. **Principle (a) – Lawfulness, Fairness and Transparency**

The College ensures that data is processed in a lawful, fair and transparent manner.

- Lawfulness
    - We don't do anything unlawful with personal data
    - We identify an appropriate lawful basis for all our personal data processing.

- If we process special category data or criminal offence data, we ensure that we identify a condition for processing this type of data.

- Fairness
  - We do not deceive or mislead people when we collect their personal data.
  - We consider how the processing may affect the individuals concerned and can justify any adverse impact.
  - We only handle personal data in ways individuals would reasonably expect, or we can explain why any unexpected processing is justified.
  - We do not deceive or mislead people when we collect their personal data.

- Transparency
  - We are open and honest with the individuals whose data we process.
  - We inform individuals through privacy notices about how their personal data will be processed, who it will be shared with and how long it will be retained.
  - We update our privacy notices when we change the purpose for processing personal data and inform individuals.

3. Principle (b) – Purpose Limitation

We ensure that we clearly identify our purposes for processing any personal data.

- We include details of our purposes in our privacy notice to individuals.
- We regularly review our processing and, where necessary, update our documentation and our privacy information for individuals.
- If we plan to use personal data for a new purpose where we have no legal obligation, we check whether the new purpose is compatible with our original purpose, and we seek specific consent for the new purpose as required.

4. Purpose (c) – Data Minimisation

We know what personal data we hold and why we need it.

- We only collect personal data we actually need for our specified purposes.
- We periodically review the data we hold and delete anything we don't need.

5. Purpose (d) – Accuracy

We ensure the accuracy of any personal data we collect, process or create.

- We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data.
- We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary.
- If we need to keep a record of a mistake, we clearly identify it as a mistake.
- Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts.
- We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data.

6. Purpose (e) – Storage Limitation

We carefully consider and can justify how long we keep personal data.

- We have a retention schedule which indicates the retention periods where possible.

- We regularly review our information and erase or anonymise personal data when we no longer need it.
- We have appropriate processes in place to comply with requests for erasure where appropriate.

7. **Purpose (f) – Integrity and Confidentiality (Security)**

We undertake an analysis of the risks presented by our processing and use this to assess the appropriate level of security we need to put in place.

- We have an information security policy and take steps to make sure the policy is implemented.
- We use encryption and/or pseudonymisation where it is appropriate to do so.
- We understand the requirements of confidentiality, integrity and availability for the personal data we process.
- We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.
- We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement.
- We ensure that any data processor we use also implements appropriate technical and organisational measures.

Retention and Deletion Policy

All Access Creative College's data is stored and deleted in line with our Data Retention Policy and Data Retention and Disposal Schedule, copies of which are available on request.

Related Documentation

- Data Retention Policy
- Data Retention and Disposal Schedule
- Learner Privacy Notice
- Workforce Privacy Notice
- General Privacy Policy

This list is non-exhaustive.

Contacts

If you have questions about this policy, please contact the Data Protection team via dataprotection@accesstomusic.ac.uk

Policy Review

This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases.

This policy will be reviewed annually.