POLICY 020

DATA ACCESS AND PROTECTION

Not a controlled document when printed

If you have a disability which makes reading this document or navigating our website difficult and you would like to receive information in an alternative format, please contact: and@acm.ac.uk

Policy_020: Data Access and Protection

1. Purpose and Scope

1.1 This policy describes how the Academy of Contemporary Music (ACM) meets its data protection obligations.

1.2 It is intended to explain in an open and accessible manner the provisions adopted by ACM to meet its data protection obligations.

1.3 This policy applies to staff, students, prospective students, alumni, and anyone else about whom ACM may have reason to collect and process data. It is designed to ensure their fair, lawful and equitable treatment in relation to the use of personal data kept by the ACM.

2. Policy Statement

Data Protection

2.1 The Academy of Contemporary Music (ACM) needs to obtain and process certain information about our students to allow us to register students, organise programmes, and to carry out other essential activities.

2.2 ACM has a need to obtain and use certain items of personal data in order to discharge our responsibilities and fulfil our obligations to educate and support our students, which could not be fulfilled without holding and using this personal data.

2.3 ACM holds and processes personal data for recruitment, admission, enrolment, the administration of programmes of study and student support and associated funding arrangements, monitoring student performance and attendance, supervision, assessment and examination, graduation, alumni relations, advisory, pastoral, health and safety, management, research, statistical and archival purposes.

The Six Principles

2.4 The General Data Protection Regulations (GDPR) ensures that Data Controllers treat data subjects and data items with an enhanced level of consideration in relating to ensuring the privacy and fair processing of the data it holds. ACM ensures that the following principles are embedded within our privacy operations:

1. Lawfulness, fairness and transparency:

Data is processed lawfully, fairly and in a transparent manner in relation to individuals.

2. Purpose limitations:

Data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3. Data minimisation:

Data held is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. Accuracy:

Data is accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5. Storage limitations:

Data kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

6. Integrity and confidentiality

Data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

General Data Protection Regulation (GDPR)

2.5 The EU GDPR replaces the Data Protection Directive 95/46/EC and is designed to standardise data privacy laws across Europe, with the intention to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy.

2.6 The following Higher Education Statistics Agency (HESA) statutory data returns include personal data as defined in the DPA and GDPR:

- Alternative Provider student record;
- The Graduate Outcomes survey (first collection 2018/19)
- Staff record;
- Student contact details may be passed to survey contractors to carry out the National Student Survey (NSS) on behalf of government agencies.

The lawful basis under the DPA and the GDPR for collecting personal data for these returns is described in the relevant Collection Notice as required by GDPR Article 13.

Collection Notices

2.7 For the purposes of data protection legislation, ACM is a Data Controller and staff, students, prospective students, alumni and others about whom we collect and process information is a Data Subject. The DPA (Principle 1) and GDPR (Article 13) require data controllers to provide information to data subjects whose data is collected that identifies data controllers and describes their purposes for processing personal data, including transfers and disclosures to other data controllers.

2.8 HESA's Collection Notices provide this information for students, staff and graduates on behalf of HESA, HESA Services Ltd, and the other organisations who are data controllers in common of HESA datasets. ACM ensures that students and staff are informed that their personal data will be submitted to HESA, and make the HESA Collection Notices available to all relevant data subjects.

The HESA Collection Notices are published at:
www.hesa.ac.uk/about/regulation/data-protection/notices

Specific data protection guidance in relation to the HESA Graduate Outcomes survey can be found here: www.hesa.ac.uk/innovation/outcomes/providers/data-protection.

Fair Collection and Processing

2.9 The specific conditions contained in Schedules 2 and 3 of the DPA regarding the fair collection and use of personal data will be fully complied with.

2.10 Individuals will be made aware that their information will be collected, and the intended use of the data specified either on collection or at the earliest opportunity following collection.

2.11 Personal data, that is data which can be connected to a specific individual, will be collected and processed only to the extent that it is needed to fulfil business needs or legal requirements.

2.12 Personal data held will be kept up to date and accurate.

2.13 Retention of personal data will be appraised and risk-assessed to determine whether business needs and legal requirements are met, with appropriate retention schedules applied.

2.14 Personal data will be processed in accordance with the rights of the individuals about whom the personal data are held.

2.15 Individuals whose personal information is held on an ACM database will be provided with the option to 'opt out' of receiving future communications.

2.16 A "cease processing" request from a data subject (often relating to unwanted communications) will be acknowledged within 3 working days, with a final response within 21 days. The final response will state whether ACM intends to comply with the request and to what extent, or will state the reasons why it is felt the requestor's notice is unjustified.

2.17 Staff will advise the nominated ACM Data Protection Officer, in the event of any intended new purposes for processing personal data. The Data Protection Officer will then arrange for a Privacy Impact Assessment to be conducted.

Security

2.18 ACM will take all reasonable technical measures to ensure the security of its network and data stored by means of its IT facilities. See also our Acceptable Use of IT and E-Safety Policy and Procedure.

2.19 Training in data protection is provided to keep staff informed of relevant legislation, guidance and best practice regarding the processing of personal information. Data protection promotes awareness of ACM's data protection and information security policies, procedures and processes. It will also promote safe practice in the use of devices off-site, handling of personal information in shared work environments and telephone conversations with third parties requesting information about data subjects.

2.20 Individual members of staff are responsible for ensuring that all personal data to which they have access is kept secure.

2.21 Staff must report any actual, near miss, or suspected data breaches to the designated Data Protection Officer for investigation. Any areas of risk identified in an investigation will be relayed to those processing information to enable any necessary or desirable improvements to be made.

2.22 Any unauthorised use of personal data collected by ACM by staff, involving the sending of sensitive or personal data to unauthorised persons or otherwise causing a breach of data protection, will be regarded as a breach of this policy. Staff disciplinary proceedings may result from wilful or negligent breaches of data protection.

Data Sharing

2.23 ACM processes applicant and student data to meet our statutory, business and other binding obligations. These include submission of statistical and data returns to the UK government and its agencies, including local authorities, the Office for Students (OfS), other official bodies, such as the Higher Education Statistics Agency (HESA), and occasional third parties carrying out contracted activities on behalf of these bodies.

2.24 In addition to the data submissions listed above, ACM may be required to provide further information to local authorities and other government agencies. This information could include learner contact details and consequently learners may be contacted separately by these local authorities or other government agencies.

2.25 Personal data in any format will not be shared with a third party organisation without a valid business reason, a Data Sharing Agreement in place, or without the consent of data subjects affected. Data Processing Agreements will be applied to all contracts and management agreements where ACM is the data controller contracting out services and processing of personal data to third parties (data processors). These agreements will clearly outline the roles and responsibilities of both the data controller and the data processor. ACM shares students' registration and academic information with the relevant validating or franchising partner institutions as part of such an arrangement, and with external examiners working on their behalf, in order to administer our courses, programmes and learning opportunities, guarantee its quality and award qualifications.

2.26 ACM may be obliged to share data with bodies such as the Police and Security Services, Her Majesty's Revenue and Customs, the Home Office and UK Border

Agency, the Department for Work and Pensions, Local Authorities, Health Authorities, and similar. These bodies may require the data for the purposes of:

- the detection or prevention of a crime;
- the apprehension or prosecution of an offender;
- the assessment or collection of any tax or duty or any imposition of a similar nature; or
- establishing whether a person is "fit to practice" in a professional context, for example in healthcare.

2.27 In certain circumstances, staff members at ACM may have a duty to disclose sensitive information about students under the age of 18, or vulnerable adults, to designated colleagues or appropriate government agencies under the terms of our Safeguarding Policy or the Prevent Duty.

2.28 ACM may be required to give information to the UK Border Agency about students, particularly those holding Tier 4 visas. Reporting duties include informing the UK Border Agency if a relevant student fails to register, withdraws from their course, or fails to attend classes and submit assignments.

2.29 ACM cannot release any information about data subjects over the age of 18 to their parents, or other sponsors, without consent (however the Data Protection Act allows disclosure without consent in certain specific circumstances). Where parents or sponsors pay tuition fees, this does not give them a right of access to students' personal information. All necessary information will be issued to the student directly. It is then the student's responsibility to pass relevant information onto their parents or sponsors.

However, students may provide consent that we in turn provide information directly to a parent or sponsor by informing Registry staff. In this event, ACM would engage directly with the third party.

2.30 Personal data will not be transferred outside the European Economic Area (EEA) unless the country or territory in question can ensure a suitable level of protection for the rights and freedoms of the data subjects in relation to the processing of their personal data.

2.31 ACM normally will not reveal personal information about students or alumni to other students or alumni except in certain specific cases of student employment with ACM, for example, students employed conducting surveys or acting as Student Ambassadors. In these situations full cognisance will be taken of data protection concerns in the relevant training and job description.

Next of Kin/Emergency Contact Details

2.32 All students are asked to provide next of kin or emergency contact details. In the event of an emergency, ACM may need to make contact with, or disclose information to, students' next of kin or other nominated emergency contact without obtaining consent. However, this information will only be used in exceptional circumstances.

Sensitive personal data/Special categories of personal data

2.33 There are particular categories of data that are categorised as 'Sensitive personal data' under the DPA and 'Special categories' under GDPR. These are subject to stricter conditions of processing. The following data fields in the HESA record capture

sensitive or special categories of personal data:

- Disability
- Ethnicity
- Gender Identity
- Religion or belief
- Sexual orientation

2.34 Collection of these sensitive or special categories of data is necessary for statistical research purposes to help public authorities to meet their public-sector equality duties under the Equality Act 2010. This processing is lawful under the Data Protection (Processing of Sensitive Personal Data) Order 2000 (Schedule (9)) and GDPR Article 9(2)(j).

Extenuating Circumstances Applications

2.35 Applications for deferred assessments, consideration of extenuating circumstances, and associated documentation may contain personal and medical information which is categorised as "sensitive personal data".

2.36 Personal sensitive data relates to racial or ethnic origins, political opinions, religious beliefs, union membership, physical or mental health (including disabilities), sexual life, and the commission or alleged commission of offences and criminal proceedings.

2.37 Since this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked via the Extenuating Circumstances forms to give express consent for ACM to do this.

Access

2.38 Members of staff will have access to personal data only where it is required as part of their functional remit.

2.39 All data subjects have a right to:

- find out what personal data ACM holds about them, why we hold it and what we do with it, how long we keep it and to whom we may disclose it;
- Ask ACM to correct inaccurate data;
- Ask ACM not to process information about students that causes them substantial, unwarranted damage or distress;
- Request a copy of their personal information held by ACM and know the source of the information;
- request information about the reasoning behind any automated decisions

This is known as a **Subject Access Request.**

2.40 ACM has 40 calendar days to comply with a student's request after receiving proof of identity, the statutory fee of £10 and any further information needed to find the information requested.

2.41 Staff are made aware that in the event of a Subject Access Request being received, their emails may be searched and relevant content disclosed, whether marked as personal or not.

2.42 Third party personal data will not be released by ACM when responding to a Subject Access Request or Freedom of Information Request (unless consent is specifically obtained, obliged to be released by law, or necessary in the public interest).

Links with the Freedom of Information Act 2000

2.43 The Freedom of Information Act 2000 (FOIA) enables greater public access to information held by public bodies and by companies receiving public funding. However, personal data continues to be protected by the Data Protection Act 1998, and is therefore exempt from disclosure under the Freedom of Information Act (Section 40).

2.44 Any FOI request for information which would involve the disclosure of third party personal information must be considered by ACM, but any decision to disclose or refuse to disclose will be made in accordance with the FOIA, and if appropriate in consultation with the person or persons whose personal information is, directly or indirectly, the subject of the request.

2.45 ACM will, as required by the FOIA, disclose information covered by the FOIA on receipt of a valid request.

Student Responsibilities

2.46 It is essential that ACM has a complete and accurate record of students' relevant personal information and course/programme details. ACM initially collects students' personal data from their application form. After enrolment, we request that students notify ACM promptly to let us know if any of this information changes during the course of the year.

2.47 Every student therefore has a responsibility to help ensure that the information held about them on ACM's student record system is correct.

Addresses and student contact details

2.48 All written communication sent by ACM will be forwarded to the address held on a student's record. During the span of a programme of study, written communications will normally be sent to a student's term-time address; before or after a programme of study. If this address is incorrect, ACM cannot be held responsible for any problems arising from the late receipt, loss of information, or receipt of information by a third party, including Induction and Registration information or Award Certificates or transcripts.

2.49 ACM contacts students via text message and will use up to date mobile telephone numbers for that purpose.

Student Email Addresses

2.50 Enrolled students receive an ACM email Account. This is for internal access only. Students and staff should not disclose another student's email address without their express permission. Staff email addresses should not be disclosed without permission except where the disclosure is reasonably covered by the staff member's professional function.

2.51 ACM will, on occasion, send emails to all students containing important academic

or administrative information, or information/advice that may be of benefit.

Students' Assessed Work

2.52 Coursework and assignments (not examination scripts) are considered to be intellectual property and the personal data and therefore the property of students. Students are advised to retain a copy of all assessed work, and are expected to obtain and make a copy of their feedback as soon as it is available.

2.53 ACM will retain coursework/assignments for a period of 1 academic year after submission for consideration by the relevant Student Progression and Achievement Boards and/or Finalist Examination Boards, and in order to meet internal academic, statutory and regulatory requirements.

2.54 After this period and without further notification, coursework and assignments will be securely destroyed.

Transcripts and Degree Certificates

2.55. Please note that ACM may withhold personal information relating to academic attainment such as transcripts and certificates where a student owes tuition fees to ACM.

2.56 Where ACM has withheld a student's transcript or degree certificate, students can request their information via a Subject Access Request (see 2.37 above). This is a request for information about you to which you are entitled under the Data Protection Act, 1998.

Retention of Information

2.57 ACM will keep a full student record for the duration of a student's studies at ACM, plus one academic year. After this time the only documentation that ACM guarantees to keep in perpetuity is a transcript of results and a standard academic reference.

2.58 Certain materials may be held for longer periods to comply with legal requirements, for quality assurance purposes, to meet professional body requirements, or the needs of a validation body. These will be held, wherever practicably and appropriately, anonymously or with the consent of the student concerned.

2.59 Archived records are securely destroyed after the appropriate length of time, in accordance with the relevant ACM record retention schedule. Please refer to ACM's Data Retention Policy for an in depth explanation of ACM's approach to Data Retention.

2.60 Archive boxes should be clearly labelled with:

1. Contents (and whether contents are confidential)
2. Disposal date

Information Commissioner's Register of Data Controllers

2.61 ACM's entry in the Information Commissioner's Register of Data Controllers can be seen by interested parties. This register entry describes, in very general terms, what personal data we process and why, how ACM obtains personal data and to

whom we may disclose it.

2.62 ACM's Registration Number is Z6627433.

2.63 ACM's nominated Data Protection Officer can be contacted via:

- DPAofficer@acm.ac.uk
- Data Protection Officer

The Academy of Contemporary Music

Rodboro Buildings

Bridge Street

Guildford

Surrey

GU1 4SB

United Kingdom

3. **Responsible Parties**

3.1 The policy lead is responsible for the cyclical monitoring and review of the policy in liaison with the Quality Assurance and Enhancement Manager. The Data Protection Policy lead is:

- ACM Data Protection Officer

3.2 All ACM staff with line management responsibility, and direct reporting staff, have a responsibility to demonstrate due regard to the Data Protection Policy.

3.3 Implementation and compliance with the Policy, overseen by the following designated staff:

- Registry Manager
- Human Resource staff
- Quality Assurance and Enhancement Manager
- Head of Information Technology
- Student Finance Officers
- Admissions Manager
- Group Head of Facilities

4. **Reference Points**

4.1 Internal:

- Quality Assurance and Enhancement Policy
- Admissions
- Acceptable Use of IT
- Equality and Diversity
- Safeguarding Policy
- Prevent Duty Policy

- Data Retention Policy

4.2 External:

- HESA Collection Notices (https://www.hesa.ac.uk/about/regulation/data-protection/notices)
- EU General Data Protection Regulation (GDPR)
- Data Protection Act 1998
- Freedom of Information Act 2000
- Education Act 2002
- Further and Higher Education Act 1992
- QAA Quality Code, Chapter C: Published Information
- CMA Guidance for HE Providers
- ICO Guide to the General Data Protection Regulation

5. **Date of Approval and Next Review**

Version: 1.3

Approved on: 15 Sep 2022

Approved by: ACM Data Protection Officer

Next Review: Aug 2023