RNCM
ROYAL NORTHERN
COLLEGE of MUSIC

Royal Northern College of Music
Data Protection Policy
Policy & Procedure
Department: Executive
Document owner: DPO (Librarian)
Approval Committee: Executive Committee
Revised: February 2018
Period of Approval: 3 years
Review Date: February 2021

1. PURPOSE

The purpose of this Policy is to ensure that the RNCM (hereinafter 'the College') and its staff and students comply with the provisions of the General Data Protection Regulation (GDPR) when processing personal data.

Compliance with the Regulation will be achieved through adherence to the principles of data protection, thus ensuring that personal data is:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary for the purposes for which it is obtained;
- accurate and up to date;
- not kept for longer than is necessary;
- processed in a manner that ensures appropriate security.

2. SCOPE

This Policy applies to all College staff, students and others who use or process any personal information on behalf of the College.

3. POLICY STATEMENT

The College is committed to protecting the rights and freedoms of individuals with respect to the processing of their personal data. The policy applies to all personal data which are held either electronically (including CCTV footage and Automatic Number Plate Recognition [ANPR] images) or in a manual filing system.

Under the terms of the GDPR, personal data is defined as

> "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic or social identity of that natural person."[1]

Measures will also be applied to ensure that special categories of personal data[2] are handled appropriately by the College. Special categories of personal data are information relating to an individual's:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic and / or biometric data;
- health;
- sex life;
- sexual orientation

Special categories of personal data can be processed only if one of the following conditions applies:

[1] GDPR Article 4(1)
[2] GDPR Article 9

- with the explicit consent of the data subject for specified purposes;
- compliance with employment and social security law, either by the College or on behalf of the data subject;
- it is necessary to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent;
- it is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents;
- the data has been made public by the data subject;
- it is necessary in relation to legal proceedings;
- it is necessary for reasons of substantial public interest;
- it is necessary for the purposes of preventive or occupational medicine;
- it is necessary for reasons of public interest in the area of public health;
- it is necessary for archiving purposes in the public interest, scientific, historical research purposes or statistical purposes in accordance with Article 89(1).

The GDPR gives the following rights to individuals (data subjects):

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure ('right to be forgotten')
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to individual decision-making, including profiling

The College is committed to upholding these rights through its policies, procedures and practices.

The College holds personal information relating to, amongst others, staff, students, visiting artists, alumni, applicants, audience members, donors, enquirers and supporters, who are defined as 'data subjects' by the GDPR. Such data must only be processed in accordance with this Policy and with the terms of the College's Notification to the Information Commissioner, which sets out the purposes for which the College holds and processes personal data. Any breach of the Policy may result in the College, as the registered Data Controller, being liable in law for the consequences of the breach. This liability may extend to the individual processing the data and his/her Head of Department under certain circumstances.

4. RESPONSIBILITIES

4.1 Senior Management

The RNCM has a corporate responsibility to implement the provisions of the GDPR, supporting a general right of access to the information in its possession and maintaining its records and record-keeping systems in accordance with the regulatory environment. The member of the College's senior management with overall responsibility for this policy is the Director of Finance and Strategic Planning. The College is accountable to the Information Commissioner in its compliance with the Regulation.

4.2 Data Protection Officer (DPO)

The DPO is responsible for drawing up guidance for the implementation of best practice and promoting compliance with the GDPR. The DPO will advise on policy and best practice and will report to the Director of Finance and Strategic Planning and Executive Committee. The Quality Assurance and Enhancement Manager (QAEM) will ensure that the notification is kept up-to-date.

4.3 Heads of Schools / Departments

Heads of Schools and Departments have a responsibility to ensure compliance with the Regulation and this Policy, and to develop and encourage good information handling practices, within their areas of responsibility.

4.4 All users

All users of personal data within the College have a responsibility to ensure that they process the data in accordance with the principles and the other conditions set down in the GDPR.

4.5 Third parties

Third parties such as consultants, contractors or agents, undertaking work on behalf of the College including personal data, must adhere to the College's Data Protection Policy and comply with the GDPR. The College remains the data controller of all personal data, including that managed under formal agreement by third parties.

5. DISCLOSURE OF PERSONAL DATA

5.1 Subject Access Request (SAR)

The GDPR gives data subjects a right to access to personal data held about them by the College. Details of how to make a subject access request are contained in the Subject Access Request Procedure. This applies to all individuals whether or not they are members of the College.

All formal subject access requests must be responded to within one month of receipt of the request, as prescribed by the Regulation, and must be notified to the QAEM as soon as they are received. Any cases of doubt as to whether a request for access to personal data is a subject access request under the Regulation must be referred to the QAEM without delay. A record must be kept of all requests for access to personal data.

Requests for transcripts of results and attainment are dealt with separately and should be directed to the Student Finance & Records Administrator in Registry.

5.2 Disclosure of personal data to others

Personal data must not be disclosed to other people or organisations, unless for legal or statutory reasons. Personal data may not be disclosed even to relatives, guardians or carers (e.g. to parents of students, including those under the age of 18, and JRNCM students) unless the data subject gave consent at the time the data was collected. If you are in any doubt as to whether it is permissible to disclose personal data, please contact the DPO for advice.

5.3 Disclosure of personal data to law enforcement agencies

Under the terms of the GDPR (Article 23) and the *Data Protection Act 2018* a limited exemption permits the College to provide personal data (including CCTV footage) to law enforcement agencies in connection with matters relating to national security and / or the prevention, detection or investigation of crime without the permission of the data subject. Any staff member in receipt of such a request should advise the QAEM and, if necessary, obtain advice on how to respond.

Any request for the disclosure of information by the College to a law enforcement agency should be made in writing – in the case of the police there is an agreed data protection form. The form must certify that the information is required for an investigation concerning national security, the prevention or detection of crime, or the apprehension or prosecution of offenders, and that the investigation would be prejudiced by a failure to disclose the information. The form should be signed by a ranking officer (usually Sergeant or above).

If the agency does not have a recognised form for the purpose, the request should be put in writing on headed notepaper and signed by an officer of the agency. It should also describe the nature of the information which is requested, the broad nature of the investigation, citing any relevant statutory authority for requesting the information and certify that the information is necessary for the investigation.

If the information is required in an emergency, the staff member taking the request should log the details of the request and the name, rank and number of the requesting police officer. If time permits, the information should be verified independently with a more senior officer. The request should be followed up with a written request from the relevant agency.

6. DATA SECURITY BREACH

In the event that personal data or other confidential information is disclosed or potentially disclosed without authorisation, either accidentally or deliberately, the member of staff discovering the breach must report it as soon as possible using the Data Security Breach Management Procedure.

7. SANCTIONS FOR BREACH OF POLICY

Users should note that depending on severity, breaches of this policy could lead to disciplinary proceedings, and could potentially constitute gross misconduct.

8. RELATED DOCUMENTS

Information Security Policy
Records Management Policy
Freedom of Information Policy
Retention Schedule
IT Policy
Data Security Breach Management Procedure
Subject Access Request Procedure

9. MONITORING AND AUDIT

This Policy and its implementation will be subject to internal monitoring and auditing.

9. CONTACT

Quality Assurance and Enhancement Manager
Royal Northern College of Music
124 Oxford Road
Manchester
M13 9RD
E: foi@rncm.ac.uk