Royal Northern College of Music

Information Security Policy

Policy & Procedure

Department: Executive

Document owner: Director of Finance

Approval Committee: Executive Committee

Revised: November 2021

Period of Approval: 3 Years

Review Date: November 2024

RNCM
ROYAL NORTHERN
COLLEGE of MUSIC

1. Purpose, scope and objectives

The RNCM (hereinafter 'the College') uses information in many forms: printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Regardless of the form it takes, or means by which it is shared or stored, information should always be protected appropriately.

This policy sets out the steps which members of the College are required to take to protect the security of all 'sensitive' information. Sensitive information (see Appendix 1)[1] is

a) personal data relating to individuals (staff, students and others), also known as Personally Identifiable Information (PII); and,
b) business information,

whose unauthorised disclosure is likely to result in damage to the interests of the individual or the College.

A breach in information security could be an infringement of the Data Protection Act 2018 and / or the General Data Protection Regulation (GDPR) and could lead to civil or criminal proceedings against the College and / or an individual. Assessing and understanding the risks will help to establish the appropriate information management processes and procedures which, in turn, should ensure appropriate incident management and recovery if security is compromised.

Information security ensures that 'sensitive' information is stored, read, edited, accessed and otherwise used only by those who have the right to do so. It is concerned with guaranteeing availability (ensuring that authorised users always have access to information when they need it), integrity (safeguarding its accuracy and completeness), confidentiality (ensuring that sensitive information is accessible only to those authorised to use it), and authenticity. It also covers proper methods of disposal of information that is no longer required.

The policy applies in particular to members of staff, but also covers students wherever appropriate. It provides a framework within which to define roles and responsibilities with respect to data security, and makes explicit the College's attitude to any actions which threaten the security of its information assets.

The objectives of the Information Security Policy are to:

- ensure that all of the College's computing facilities, programs, data, network and equipment are adequately protected against loss, misuse or abuse, and that this protection is cost-effective;
- ensure that all users are aware of, and fully comply with, this policy statement and all associated policies and procedures;
- ensure that paper records are kept securely and managed effectively;
- ensure awareness of appropriate security measures that must be implemented as part of the effective operation and support of information management systems;
- ensure that information is disposed of in an appropriate, secure, manner when it is no longer relevant or required.

Those requiring further information, explanation or training about any aspects of the policy which relate to computer security should discuss their needs with the IT Department. Questions about the creation, classification, retention and disposal of records (in all formats) should be directed to the Data Protection Officer (DPO).

[1] Note that this use of the word 'sensitive' is different from that in the DPA 1998 referring to 'sensitive personal data'. This description has been amended in the GDPR to 'special categories of personal data'.

2. Compliance

College staff and students have an obligation to abide by all relevant legislation. Of particular importance in this respect are the Computer Misuse Act 1990, the Data Protection Act 2018, the Freedom of Information Act 2000, Human Rights Act 1998, the Counter Terrorism and Security Act 2015 and the General Data Protection Regulation.

3. Roles and responsibilities

Users of College systems and information have responsibility for protecting information assets. Failure of an individual student or member of staff to comply with this policy may lead to the instigation of disciplinary procedures and, in certain circumstances, legal action may be taken.

3.1 Data Protection Officer (DPO)

The DPO (Head of Library Services) advises the College and users about their obligations to comply with the general data protection regulations and other data protection laws. The DPO monitors compliance, including managing internal data protection activities, advises on data protection impact assessments, trains staff and conducts internal audits. The DPO is the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers, etc.).
In addition, the DPO is responsible for developing the policy for records management and providing advice and guidance. Operational responsibility for records management is delegated to Heads of Departments / Schools / Programmes to implement procedures and promote compliance.

3.2 Head of IT (HIT)

HIT is responsible for managing the IT infrastructure, ensuring the security of systems and servers, and controlling access to those systems.

3.3 Specific data leads

There are a number of specific data leads with responsibilities as follows:

Data type	Responsible
Employees (prospective, current and archive)	Head of Human Resources / Head of Business Systems and Data Unit
Students (current and archive)	Academic Registrar ; Head of Business Systems Data Unit
JRNCM students (current and archive)	Head of Junior RNCM
Finance and Payroll (current and archive)	Deputy Director of Finance (Management Information)
Alumni, donors and supporters (current and archive)	Director of Development
Audience members, customers (including ticket purchase), enquirers, prospective students and applicants	Head of Marketing and Communications
Commercial contracts and tenders	Director of Finance
Library users	Head of Library Services

3.4 Heads of Departments / Schools / Programmes

Heads of Departments, Schools and Programmes are required to implement this policy in respect of both paper and electronic systems operated by their area and are responsible for ensuring that staff, students and other persons authorised to use those systems are aware of and comply with it and associated procedures.

Staff with supervisory responsibility should ensure that their supervised staff or students are aware of best practice with regard to information security.

3.5 All users

Individuals must, at all times, act in a responsible and professional way and must refrain from any activity that may jeopardise security. Users will be assigned with usernames and passwords for RNCM systems. It is the responsibility of users to keep these passwords secret and secure, and to let the IT department know immediately if they have reason to suspect somebody else may know their passwords (for instance if a user has fallen victim to a phishing attack).
Users are responsible for any conduct that occurs through use of their username/password.

Users must be mindful of the reputational and legal risks of any data loss, and take all sensible precautions to avoid such loss. Typically this would involve storing data/documents only on College servers or College OneDrive/SharePoint, and taking reasonable precautions to ensure any computer they use to access College data (e.g. home computers, internet cafes) is secure.
Users are expected to adhere to the IT Policy which specifies in detail the responsibilities of users of data, how data should be securely accessed, stored and deleted.

- Policies: Comply with the College's policies as specified in section 6.

- Security - electronic: Assess the sensitivity of all information created and received; and take proportionate measures to ensure that data are held securely (including access to the website). This includes appropriate use of passwords, PIN, encryption, etc. when using portable or fixed devices, whether owned by the College or not. Users should ensure that no unauthorised person can access computers which are left logged on and unattended.

  Sensitive data must ***only*** be stored on College-owned fixed or portable devices that are encrypted, e.g. encrypted laptops and memory sticks.

- Bring your own device (BYOD): If a non-College computer is used to create or access sensitive information, users must ensure that the computer has up-to-date security protection, and that no-one else can use it to view College information. Data must transferred securely to a College-owned device and any data held on the non-College device must be deleted after use (including removal from any temporary or trash files).

- Security - paper: All paper records containing personal information, e.g. student or staff files, must be stored in lockable cabinets, cupboards or drawers. This storage furniture should not be left unlocked if an office or other room is left unattended for a period of time and could be accessed by others who do not have permission to view the information. No personal data should be left accessible on desks overnight.

  Save in very exceptional circumstances highly confidential paper documents should not be taken outside the College; if this is necessary they should be stored securely (locked cabinet, secure briefcase kept with the user) at all times.

- Data sharing: Sensitive information may be shared only where the conduct of College business requires this, where it is allowed within the law or where the data subject has given specific consent.
  When emailing sensitive information to other members of the College, always use the College email address, not a personal one. Ensure the correct address is used before sending the email.

- Remote access: When off campus (i.e. using remote access) to access College e-mail or data, either use links provided via the College website, intranet and Moodle or, if mobile devices are used for this purpose, make sure they are password or PIN protected, or otherwise encrypted. Do not set up passwords which are then automatically remembered by the device for future use if on a non-College owned machine (e.g. home device, internet café, open Wi-Fi, etc.).

- Web services: Unapproved third party web services, e.g. Dropbox, must NOT be used for storing, processing and transferring data which is (a) sensitive [defined in appendix 1]; (b) of such criticality that functions or operations would be disrupted should it be lost or become unavailable or corrupted [see Business Continuity Plan]; or (c) market sensitive information [as agreed by the Director of Finance].

  Personal data must be stored only on servers hosted in EU, or using a supplier whose services comply with the EU-U.S. Privacy Shield Framework[2] and thus with the GDPR.

- Safe disposal: Use shredding machines or College-approved shredding services for disposal of classified paper documents. Any unwanted, damaged or obsolete computer hardware must be disposed of through the IT Department.

4. Information assets and classification

Those using or storing data should refer to the classification of data table in Appendix 1 to assess the value of information handled, its sensitivity and the appropriateness of security controls in place or planned.

5. Incident management

Incidents involving information assets may take the form of security breaches or a loss of access resulting in the implementation of the College's business continuity plan. Critical data functions are articulated in the plan and have specific recovery plans and times.

5.1 Breaches of security

Any member of staff who is aware that they or someone else has, or may have, lost personal data or caused it to be accessed without authorisation is obliged to report the breach as soon as it is discovered.

Full details on what to do in this event are in the Data Security Breach Management Procedure which is available on the intranet.

5.2 Business continuity

As part of business continuity plans, arrangements are in place to ensure security of personal data.

[2] http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_en.pdf

6. Related Documents

- Data Protection Policy
- Data Security Breach Management Procedure
- Records Management Policy
- Retention Schedule
- IT Policy
- Mobile Communications Policy
- Privacy Notices
- Social Media Policy [staff]
- Social Media Protocol [students]

Information Classification Scheme

Class	Rationale	Examples
Open	Information considered 'public' or 'unclassified' and which may be seen by anyone Access to open information is unrestricted. May include: • Anonymised data • Data where subject has given permission for data to be put into the public domain • Information available from publicly available bodies or regulatory bodies	• Prospectus, programme and course information • Published reports • Staff directories with names and contact details • Press releases (not under embargo) • Open content on the RNCM web site • Publicity information • Researcher profiles and publications • Policies and procedures (excluding those containing security-related information) • Events programmes with biographical information • Photographic images • Publication of final degree result
Private	Information where dissemination is normally restricted Access to private information is normally restricted and governed by appropriate policies or contracts.	• Teaching materials • Exam papers (post--examination) • Class lists • Draft press releases • Current procurement information • Committee minutes
Confidential	Information which is sensitive. Dissemination is normally prohibited except within strictly defined and limited circumstances. Such information is likely to include personal data, commercially sensitive or legally privileged information, or information currently under embargo. Unauthorised disclosure of this information could: • Cause damage or distress to individuals • Breach undertakings to maintain the confidence of information provided by third parties • Breach statutory restrictions on the use, or disclosure, of information • Breach contractual agreements	• Student personal details (including JRNCM, Young Strings, Young Projects, Participants in RNCM Engage) • Staff personal details • Personal details of others, such as donors, audience members • Exam papers (pre-examination) • Student assessment results and feedback • Financial transactions • Internal reports • Reserved Committee business • Commercial and research contracts • Procurement and tender information • Restricted research data • Research grant applications

Class	Rationale	Examples
	• Breach a duty of confidentiality or care • Cause financial loss or loss of earning potential to the College • Disadvantage the College in commercial or policy negotiations with others • Prejudice the investigation or facilitate the commission of crime	• Legally privileged information, including legal advice • Information where release would result in a breach of confidence