Royal Conservatoire of Scotland

Data Protection Policy

Document Revision History

Version No.	Version Date	Prepared By	Approved By	Summary
1.1	August 2012	Caroline Cochrane	Caroline Cochrane	RCS Data Protection Policy
1.2	August 2015		C.Cochrane	Alumni inclusion
1.3	May 2018	C. Cochrane	C. Cochrane	GDPR Update
1.4	Jan 2020	M. Crowther	C. Cochrane	Text Update
1.5	Mar 2020	M. Crowther	C. Cochrane	Age of Legal Capacity Update

Data Protection Policy

1. Introduction

In order for The Royal Conservatoire of Scotland (RCS) to deliver its core learning and teaching functions, operate effectively as a business and performing arts venue and meet legislative, contractual and statutory obligations, it needs to process personal data relating to present, past and prospective stakeholders in order to comply with the requirements of the General Data Protection Regulation (GDPR). As our recording and processing of data continues to increase, it is more important than ever that every member of RCS staff understands the laws that exists in relation to data protection, and their responsibilities in ensuring that data is secured and protected in line with the law. This Policy should be read in conjunction with the RCS Information Security Policy.

2. Definition of "Personal Data"

The GDPR applies to "personal data," meaning any information relating to an identifiable person who can be directly or indirectly identified by that data. For example, this could include name, address, e-mail address, date of birth, national insurance number etc. In order to reflect technological changes, GDPR also defines personal data to include elements such as location data or other online identifiers such as IP address.

"Special Category" (SC) data is personal data which the GDPR identifies as more sensitive, and so requires further protection. This SC data can include identifiers such as race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation.

3. Scope

This policy applies to all those individuals and organisations that process personal data on behalf of the RCS, including but not limited to:

- Employees, consultants, contractors and temporary staff
- Students undertaking credit bearing and non-credit bearing programmes of study offered by the RCS
- Suppliers and partners of the RCS
- Other third parties associated with the RCS

4. Policy Statement

This policy helps provide a demonstrable commitment to, and support of, compliance with data protection legislation by the RCS and supports the RCS's core functions, which are reliant upon accurate, available and usable personal data and the trust of RCS stakeholders. Compliance with data protection legislation also enables efficient working practices and significantly reduces the likelihood of an information security breach and its wider effects including causing harm or distress to data subjects, reputational damage, potential fines and any further undertakings from the Information Commissioner.

The RCS is committed to protecting the rights and freedoms of individuals in accordance with the provisions of data protection legislation. In order to achieve this, the RCS shall ensure that personal data is handled appropriately, consistently and securely.

RCS shall ensure that personal data is:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date; every reasonable step shall 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
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed
- 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

5. The Data Controller

The Royal Conservatoire of Scotland, as a data controller, shall be responsible for, and be able to demonstrate, compliance with the principles of data protection legislation. The RCS will appoint a Data Protection Officer (DPO) to assist the RCS to monitor internal compliance, inform and advise on our data protection obligations, and act as a contact point for data subjects and the supervisory authority. The RCS's named DPO is Lisa Powell, who can be contacted at dataprotection@rcs.ac.uk

6. Collecting and Sharing of Personal Data

Ensuring that personal data is collected and shared appropriately is vital to the successful operation and the reputation of the RCS, and for maintaining the trust of our employees, students and other stakeholders. In order to achieve this, RCS shall:

- Undertake a data protection impact assessment for any new initiatives that involve the collecting and sharing of personal data where sharing is likely to result in a high risk to the rights and freedoms of people (particularly where new technology is involved)
- Identify a lawful basis in data protection legislation for collecting and sharing personal data
- Ensure that the collecting and sharing of personal data is necessary to achieve the identified objective(s).
- Collect, process and share the minimum amount of personal data required to achieve the objective(s)
- Use anonymised or pseudonymised data where the identification of data subjects is not required for the purpose of processing
- Provide data subjects with privacy notices and clear guidance on how to exercise their rights. The RCS Privacy Notices can be found at rcs.ac.uk/policy/privacy
- Record all decisions to share personal data with external partners
- Ensure that a data sharing arrangement is in place where personal data is shared with external partners on a systematic basis or there is a large scale transfer of personal data
- Ensure that data is not transferred to a country outside the European Economic Area, unless that country has an adequate level of protection for personal data

7. Conditions for Processing Personal Data

Personal data can only be lawfully processed if the processing is deemed necessary under one of the following circumstances (Lawful Basis)

- In the performance of a **contract**, e.g., staff contract or student enrolment contract
- In compliance with a **legal obligation**
- In the performance of a **public task**
- In the **legitimate interests** of the data controller, unless prejudicial to the interests of the individual
- To protect of the data subject's **vital interests**
- With the **consent** of the individual

All processing of personal data in the RCS will fall under one of these lawful bases and that lawful basis must be recorded for processing to be carried out lawfully. Additionally, RCS may process special category information, which will necessitate additional safeguards. Before processing special category information, RCS will have recorded decisions about why it is necessary and assigned a lawful basis for processing.

It should be noted that children aged 12 and over, have the right to be informed and manage their own data. The same lawful bases as listed above also apply to children. (For children under 12, parental consent to process is required). When processing data for children and relying on consent, reasonable efforts (taking into account the available technology and the risks inherent in the processing) must be taken to ensure that anyone who provides their own consent is 12 years old or older, or that the person providing consent holds parental responsibility for the child.

8. Obligations and Responsibilities of Staff

All staff are obliged to:

- Ensure that any information they provide to RCS in connection with their employment is accurate and up-to-date, and inform the Human Resources Department of any changes to their information, e.g., address, contact details for next of kin, etc.
- Provide information in response to Data Protection audits and data breach investigations
- In the event of a subject access request, provide all relevant information to the DPO
- Undertake training on Data Protection and Information Security

Directors and Heads of Departments are responsible for ensuring that their staff are acquainted with the requirements of data protection legislation. Data Protection training will be mandatory for all staff who handle personal data as part of their job. Guidance, advice and support can be sought directly from the Head of Information Services.

All staff are responsible for ensuring that:

- Any personal data which they hold are kept securely and for only as long as is necessary (in accordance with the RCS Records Retention Schedule)

- Personal data is not disclosed either orally or in writing, accidentally or otherwise to any third party, without authorisation

Staff should note that unauthorised disclosures will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

All staff should ensure that personal data is:

- when kept in hardcopy, is kept in a locked filing cabinet, drawer, cupboard or room
- not visible to anyone not authorised to see it, either on desks or on computer screens
- stored on private network folders and if appropriate, password protected
- be sent in a sealed envelope, if transmitted through the post, whether internally or externally
- not sent via e-mail without password protection or encryption, if it contains special category personal data
- not put on laptops, flash drives, or other portable media

NB. Staff should always choose to work with personal data onsite, but if work must be made available offsite, staff should work with data using OneDrive and/or a VPN (Virtual Private Network) to access any documents or files.

Staff should ensure that all notes/annotations/feedback/comments are suitable and don't record unsubstantiated opinions, derogatory remarks or anything else that cannot be justified and shared with the student, should it be requested.

9. Obligations and Responsibilities of Students

Students must ensure that all personal data provided to RCS are accurate and up to date. They must ensure that changes to their personal data, for example, address, name, or contact details, are notified to the Academic Administration and Support department. Students who handle personal data as part of the studies, should be aware of their responsibilities as outlined in this policy, keeping any personal data that they handle secure and confidential at all times.

10. Subject Rights and Subject Access Requests (SARS)

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object

- Rights in relation to automated decision making and profiling

Everyone has the right of access to personal data that is being kept about them. Any person who wishes to exercise this right in connection to personal data held by the RCS should make this request via dataprotection@rcs.ac.uk with details of the information requested, and proof of identification. RCS will reply within one calendar month.

11. Security and Retention of Data

All records, whether electronic or manual, must be held securely so as to prevent unauthorised or unlawful processing or disclosure of data. Appropriate measures should be taken to minimise the possibility of accidental loss, destruction or damage to personal data. To this end, staff should refrain from storing or holding Conservatoire data on their personal equipment or mobile storage devices.

Access to data must be limited to legitimate users only. Access to electronic records will be controlled through password protection and varying levels of access. Manual records will be stored securely and access to them will be controlled by a designated individual. Both paper and electronic records should be kept in accordance with the RCS Records Retention Schedule. Records will only be kept for as long as necessary and then securely destroyed.

12. Breach Reporting

A personal data breach is defined as: “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data”.

The RCS is responsible for ensuring appropriate and proportionate security for the personal data that we hold. RCS makes every effort to avoid personal data breaches, however, it is possible that data breaches will occur. Examples of personal data breaches include:

- Loss or theft of data or equipment
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Unauthorised disclosure (e.g. email sent to the incorrect recipient)
- Human error
- Hacking attack

If a data protection breach occurs, the RCS is required in most circumstances to report this as soon as possible to the Information Commissioner’s Office, and not later than 72 hours after becoming aware of it. All breaches of this policy and data protection legislation must be reported immediately to the Head of Information Services and the DPO, via the designated data protection email address dataprotection@rcs.ac.uk. Third parties shall report via their RCS point of contact. A breach of this policy by an employee or student may result in disciplinary action. A breach by a third party may result in a termination of contract.

13. Impact of non-compliance

All staff and students of RCS are required to comply with this Data Protection Policy, the supporting guidance and the requirements specified in the GDPR. Any member of staff or student who is found to have made an unauthorised disclosure of personal information or breached the terms of this

Policy may be subject to disciplinary action. Staff may also incur criminal liability if they knowingly or recklessly obtain and/or disclose personal information without the consent of the RCS i.e. for their own purposes, which are outside the legitimate purposes of the RCS. The RCS could be fined for non-compliance with the GDPR.

14. Data Protection contacts

The RCS's named Data Protection Officer is Lisa Powell. In the first instance, all enquiries or requests for further information or guidance relating to data protection should be addressed to the Head of Information Services, Caroline Cochrane, or sent to dataprotection@rcs.ac.uk