

Policy name: Privacy Policy

Approved: 25th November 2016

Revision 1 approved 10th March 2017

Revision 2 approved

Revision 3 approved by Trinity Academic Council 13th May 2020

1. Context

- 1.1 This is a statement of the practices of the Royal Irish Academy of Music, hereinafter referred to as RIAM or the Academy, in connection with the capture and use of personal data and the steps taken by RIAM to protect the individual's personal data and respect his/her right to privacy.
- 1.2 RIAM fully respects the individual's right to privacy and actively seeks to preserve the privacy rights of all staff, students and customers who share information with the institution.
- 1.3 Any personal information which is volunteered to RIAM will be treated with the highest standards of security and confidentiality, in accordance with Irish and European Data Protection legislation. RIAM will process all personal data in accordance with the [General Data Protection Regulation \(EU\) 2016/679](#) (GDPR) and the [Data Protection Act 2018](#).

2. Purpose

- 2.1 This policy describes RIAM's commitment to protect the rights and privacy of individuals in accordance with the GDPR, the Data Protection Act 2018 and related legislative frameworks (see [Appendix](#) for details).
- 2.2 This policy explains the purpose and legal basis for gathering personal data, how RIAM collects and uses personal data, how it stores and secures personal data and details of third parties with whom it shares personal data. It also outlines how to contact RIAM if any query or concern about personal information arises.

3. Scope

- 3.1 This privacy policy applies to all RIAM staff, students, users of RIAM web assets and online services, and approved third parties.
- 3.2 Within the context of this statement, personal data is defined by the Data Protection Commission as *'data relating to a living individual who can be identified either from the data alone or from the data in conjunction with other information that is in, or is likely to come into, the possession of the Data Controller.'*

4. Benefits

- 4.1 This privacy policy provides a framework in which personal data is gathered, processed and stored legally and fairly, and in keeping with the principles of data protection.
- 4.2 It establishes the terms of reference which ensure uniform implementation of data protection controls throughout RIAM.
- 4.3 It also helps to safeguard the rights of all staff, students and users of RIAM services.

5. Principles

- 5.1 RIAM undertakes to ensure that all personal data collected will be processed on the basis of either the consent of an individual concerned or another legal basis as set out in the [General Data Protection Regulation \(EU\) 2016/679](#) (GDPR) and the [Data Protection Act 2018](#).
- 5.2 All personal data will be collected for specified, explicit and legitimate purposes and will not be 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.
- 5.3 All personal data gathered will be processed lawfully, fairly and in a transparent manner in relation to the individuals concerned.
- 5.4 All personal data will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- 5.5 All personal data will be kept accurate, up to date and available for authorised use; every reasonable step will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.
- 5.6 All personal data will be 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.
- 5.7 RIAM will not store customers' credit card details. All online application services are integrated with the Global Payments/Realex Hosted Page facility which is a secure payment processing system that is fully Payment Card Industry Data Security Standard (PCI DSS) compliant.
- 5.8 Personal data may be stored for longer periods if they are required for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes. Retention of such data will be subject to the implementation of the appropriate technical and organisational measures required by the GDPR, in order to safeguard the rights of the individuals concerned.
- 5.9 RIAM will restrict access to personal data to relevant authorised personnel only. Physical, electronic, and procedural safeguards will be applied where appropriate.
- 5.10 RIAM will not sell any personal data collected to third parties for marketing or other purposes.
- 5.11 Some website pages may contain links to other websites that are not operated by RIAM. RIAM does not share users' personal data with those websites.
- 5.12 While RIAM tries to link only to sites that share its high standards and respect for privacy, it is not responsible for the content, security, or privacy practices employed by other sites and expressly disclaims all liability associated with an individual's use of such other sites and the content found there.
- 5.13 Security measures will be implemented by all RIAM users (i.e. staff, third level students and stakeholders) when processing personal data to ensure that it is protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

- 5.14 All RIAM users must understand their own responsibilities for respecting the privacy of individuals and be aware of and fully comply with the relevant Irish and European Community legislation.

6. Policy

6.1 How and Why the RIAM collects Personal Data

- 6.1.1 Personal data collected will be collected by RIAM for legitimate business reasons only and will be processed in accordance with the principles outlined in this privacy policy.
- 6.1.2 Personal data will be gathered via website forms, written application forms and documents, email, telephone queries, questionnaires and surveys.
- 6.1.3 RIAM will also collect information via third parties such as the [Central Applications Office](#) (CAO) which processes applications to undergraduate courses in Higher Education Institutions (HEIs) in Ireland.

6.2 Staff Data

- 6.2.1 RIAM collects personal data for the purposes of recruitment and for the formation and administration of employment and employee relationship.

6.3 Internal Student Data

- 6.3.1 RIAM processes data relating to part-time and third level students for admission, registration, academic assessment, supervision, monitoring, and the provision of services.

6.4 External Examination Candidates

- 6.4.1 RIAM collects personal data on examination applicants and candidates through online and manual application forms. This data is held purely for the purpose of processing examination applications so that administrators and authorised back office users can view applicant/application history as and when required. The contact information provided in online and paper application forms is used by RIAM administration to ensure that examination schedules, results and examination certificates are forwarded to the correct address. In the event of any problems or complications with examination entries, this information may also be used to contact the applicant concerned. RIAM keeps accurate records of applicant and candidate examination history in order to provide a quicker and more effective service to examination applicants.
- 6.4.2 RIAM needs to collect and process relevant information about young people if they wish to be entered for examinations and competitions, or wish to attend events or sign up to receive or use some of its services. If candidates are under 18 years, they must obtain their parent/guardian's permission before providing their personal details to RIAM.

6.5 Special Needs Examination Candidates

6.5.1 RIAM requests that examination applicants supply information on requirements for their Special Educational Needs (SEN) candidates. This may require supporting health and medical evidence to ensure that RIAM makes the appropriate adjustments for these candidates in advance of the examination day. Examination candidates must actively give consent to RIAM to retain any supporting evidence for reasonable adjustments for five years. If candidates choose not to give permission to RIAM to retain supporting evidence, or they do not respond to the request for ongoing consent, RIAM will retain the supporting evidence only for the duration of the current session (a maximum of six months from the closing date for the examination session) and these candidates will need to resubmit supporting evidence for any future examinations requiring reasonable adjustments.

6.6 Members of the Public and Consumers

6.6.1 RIAM gathers information from members of the public in order to respond to enquiries, process transactions, administer services and accept bookings for events.

6.6.2 RIAM may add an individual's name to a relevant mailing list if he/she has specifically requested to be added to the list in order to receive information which is of interest to them.

6.6.3 If an individual's data is recorded on a mailing list he/she will be provided with the opportunity to opt out from the outset and the address will only be used to forward information relevant to the initial enquiry or transaction.

6.7 Direct Marketing

6.7.1 Direct Marketing consists of contacting an individual with information about products or services, and asking them to exchange their money, data, or time. RIAM Direct Marketing can take the form of emails, text messages, post and use of OTT services (Twitter, Facebook, WhatsApp, Skype etc.).

6.7.2 Direct Marketing is a legitimate business interest under the GDPR and the ePrivacy Directive. RIAM will ensure that it meets the following criteria when promoting its services to the public:

- (i) the individual has explicitly consented to their data being processed;
- (ii) personal data is lawfully and transparently obtained;
- (iii) the intention to conduct direct marketing and reason for the campaign are made clear to the individual in advance;
- (iv) it is easy and free for an individual to opt-out (e.g. tick box on flyer).

6.7.3 RIAM will explain clearly on promotional material (e.g. flyers) a) how personal data collected is processed and secured and b) how customers may unsubscribe at any time and c) an email contact to address their concerns.

6.7.4 RIAM will sometimes offer discounts and promotional offers on tickets etc. to members of the public and may give special consideration to subscribed service users.

6.8 Types of Personal Data Collected

6.8.1 The personal data that RIAM collects comprises:

- (i) name, date of birth and gender;
- (ii) contact details (postal address, email address, landline, mobile phone number and communication reference);
- (iii) personnel/employment files;
- (iv) medical records;
- (v) financial information including transaction history (RIAM never stores credit card payment details);
- (vi) recordings of telephone conversations;
- (vii) email messages;
- (viii) image and likeness (as captured on RIAM CCTV cameras and in photographs and videos used for promotional purposes);
- (ix) applications (for internal part-time and third level courses and external examinations);
- (x) special needs information (disabilities, wheelchair access, etc.);
- (xi) records of websites visited (e.g. traffic data, location data, operating system, browser usage, and resources accessed). RIAM employs industry-wide technology called "cookies" and web beacons (small pieces of non-identifiable data that are placed on users' storage drives when they access websites). This cookie is only stored in the browser memory while visiting the website. It automatically deletes itself after several minutes of inactivity on the site or immediately on closing the browser and there is no record of the cookies stored on the user's computer. Cookies help RIAM to study traffic patterns on its websites in order to improve website performance, to customise the user experience, and to better match the users' interests and preferences. This data helps the RIAM to understand its customers and improve online facilities and how they are used. By using the RIAM website, users agree that these types of cookies may be placed on their device. The browser will give them the option of preventing websites using cookies, or deleting cookies that have been accepted. The browser's help service or help manual will show how this is done. If users do not wish their browser to accept cookies, they can "turn off" the cookie acceptance setting on the browser setting. However, they must note that this may stop the website from working properly on their devices. If users do not change their browser settings to refuse cookies, the website will issue cookies when they visit it. If users continue to use the website, they agree and consent to the use of cookies on their devices.

- (xii) the user's IP address. This is a number that is assigned to a computer automatically when the internet is used. When a user visits any web page on RIAM's website, its servers log their IP address. This IP address may be used to help diagnose problems with RIAM's server and to administer its website, and also to help identify the user and to gather broad demographic information.

6.9 How RIAM stores and secures Personal Data

- 6.9.1 The personal data collected by RIAM will be stored confidentially and securely as required by the Information and Communications Technology Policy. RIAM is committed to ensuring that all accesses to, uses of, and processing of personal data is performed in a secure manner.
- 6.9.2 In line with data protection principles RIAM will only store personal data for as long as it is necessary and in accordance with the Records Management and Retention Policy.
- 6.9.3 Personal data will primarily be stored either on premise behind a strong firewall, in encrypted format on a cloud database server, or in secure IT platforms within the European Economic Area (EEA) which are also subject to GDPR requirements.
- 6.9.4 RIAM intends to protect all personal data and to maintain its quality.
- 6.9.5 RIAM will use all reasonable efforts to take all appropriate technical and organisational measures and precautions to keep personal data secure and protected from unauthorised access, use or alteration and unlawful destruction.
- 6.9.6 Secure Sockets Layer (SSL) encryption will be applied when collecting or transferring sensitive data. SSL encryption is designed to make the data unreadable by anyone other than the intended recipient.

6.10 Sharing Data with Third Parties

- 6.10.1 RIAM will not disclose personal data to third parties without consent of the user, except in the following cases:
 - (i) Personal data may be disclosed to sub-contracting third parties to enable the performance of contracts. For instance, RIAM engages companies to perform functions on its behalf, such as processing bookings, delivering packages, sending postal mail and emails, providing marketing assistance, processing credit card payments and providing customer services.
 - (ii) Such third parties will have access to personal data required to perform these functions, but may not use it for any other purpose and are obliged to process the data in accordance with applicable law.
 - (iii) Personal data may be disclosed to third parties to enable compliance with legal obligations to which RIAM is subject. If personal data is disclosed to third parties to enable them to provide services for, on behalf of, or under RIAM's direction, then it will take measures to ensure that these third parties comply with this privacy policy, and that such recipients:

- do not use the personal data for any other purposes than those permitted by the terms of the contract;
 - obtain and process personal data only on condition that they protect that personal data from unauthorised use and adopt and comply with policies and terms concerning personal data protection and use;
 - comply strictly with applicable laws (i.e. GDPR and the Data Protection Act 2018).
- (iv) Anonymous or generic data from which an individual cannot be identified are excluded from use, processing, disclosure, transmission and other personal data use restrictions.

6.10.2 RIAM may share personal data with the following categories of third parties:

- (i) State or regulatory bodies including the Higher Education Authority, the [Central Applications Office](#) (CAO), Department of Education and Skills, Department of Justice and Equality, Department of Social Protection.
- (ii) ICT or cloud service providers that provide essential services to RIAM e.g. Microsoft.
- (iii) Firms that provide professional services to RIAM such as legal firms and auditors.
- (iv) Firms that provide archiving, storage or disposal of confidential waste.
- (v) Schools etc. that provide work placements for students.
- (vi) An Garda Síochána when RIAM is required by law to do so.

6.10.3 RIAM will endeavour to share only the data that is needed and ensure that the data are processed according to its specific instructions, and that the same standards of confidentiality and security are maintained throughout the operation. Once the processing of the data have been completed third parties will be required to return the data to the RIAM except where they are required to retain it by law.

6.11 Right of Access to Personal Data

6.11.1 Individuals have the right to access their personal data, and to rectify or delete inaccuracies in their personal data, and to object to the processing of their personal data.

6.11.2 If a user would like to view their personal data stored in RIAM's database, he/she should contact the Data Controller.

6.11.3 For privacy protection reasons, an individual requesting their personal data will be asked to provide some proof of identification.

6.11.4 On demand, users can receive an explanation regarding the processing of their personal data and also obtain confirmation that all relevant parties have been notified of their request(s) for information, for alteration or for deletion, as appropriate. RIAM will seek to comply with such requests.

6.11.5 If a user would like to unsubscribe from an email sent to them, they should contact the relevant department or the [Data Controller](#).

6.12 *Right of Rectification or Erasure*

6.12.1 Under the GDPR and Data Protection Act 2018, RIAM staff, students and stakeholders have the right to have their personal data corrected, if inaccurate, or erased, if there is not a legitimate reason for retaining the data.

6.12.2 A request for rectification or erasure should be made in writing to the Data Controller, outlining the data in question and the reason why this personal data should be updated or erased.

7. Responsibility

7.1 RIAM has overall responsibility for ensuring compliance with data protection legislation where it is the controller of personal data.

7.2 The RIAM Secretary is responsible for overseeing this policy and its operational procedures, however, all staff and students of RIAM who collect and/or control the contents and use of personal data are individually responsible for compliance with the data protection legislation.

7.3 RIAM will provide support, assistance, advice and training to all departments, offices and staff to ensure it is in a position to comply with the legislation.

7.4 *Contact Details*

Data Controller: Kevin Kelleher at email: kevinkelleher@riam.ie

Data Protection Officer: Theresa Doyle at email: theresadoyle@riam.ie

8. Legislation and Regulation

8.1 [General Data Protection Regulation \(GDPR\)](#).

8.2 [Data Protection Act 2018](#).

9. Related Documents

9.1 Data Protection Policy.

9.2 Information and Communications Technology Policy.

9.3 Records Management and Retention Policy.

9.4 Closed Circuit Television Policy.

9.5 Privacy Statement.

9.6 Social Media Policy.

10. Document Control

Approved by Board of Studies 25th November 2016.

Revision 1 approved by Board of Studies 10th March 2017.

Revision 2 approved.

Revision 3 approved by Trinity Academic Council 13th May 2020.

Next review: Academic year 2020/21.

Appendix - General Data Protection Regulation

1. The [General Data Protection Regulation](#) (GDPR) came into force on the 25th May 2018. An accompanying Directive establishes data protection standards in the area of criminal offences and penalties. This is known as the [Law Enforcement Directive](#).
 2. The GDPR and the Law Enforcement Directive provide for significant reforms to current data protection rules. This legislation emphasises transparency, security and accountability by data controllers and processors, while at the same time standardising and strengthening the right of European citizens to data privacy. It also increases the range of possible sanctions for infringements of these rules.
 3. Although the GDPR is directly applicable as a law in all Member States, it allows for certain issues to be given further effect in national law. In Ireland, the national law, which, amongst other things, gives further effect to the GDPR, is the [Data Protection Act 2018](#).
 4. Data Protection is the safeguarding of the privacy rights of individuals in relation to the processing of personal data, in both paper and electronic format. The terms of the **Data Protection Act 2018** lay down strict rules about the way in which personal data are collected, accessed, used and disclosed. The terms of the legislation also permit individuals to access their personal data on request, and confer on individuals the right to have their personal data amended if found to be incorrect.
 5. The Data Protection Commission (DPC) derives its regulatory authority to protect individuals' data protection rights from a number of legislative frameworks which comprise:
 - (i) the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679);
 - (ii) the Data Protection Act 2018;
 - (iii) the "Law Enforcement Directive" (Directive (EU) 2016/680) which has been transposed into Irish law by way of the Data Protection Act 2018;
 - (iv) the Data Protection Acts 1988 and 2003;
 - (v) the 2011 "e-Privacy Regulations" ([S.I. No. 336 of 2011](#) – the European Communities (Electronic Communications Networks And Services) (Privacy And Electronic Communications) Regulations 2011).
- For further details please refer to the Data Protection Commission (DPC) at URL: <https://www.dataprotection.ie/docs/GDPR/1623.htm>
6. The DPC has launched a GDPR-specific website www.GDPRandYou.ie with guidance to help individuals and organisations become more aware of their enhanced rights and responsibilities under the General Data Protection Regulation.
 7. Advice on GDPR matters is also available from the [Citizens Information Board](#).