Information Management Policy & Procedures

1. Introduction and legal context

1.1. The Royal Academy of Dance (RAD) collects, processes stores and shares information about its employees, members, registered teachers, students, candidates, customers and other contacts, (referred to in this policy as "Individuals") in order to operate its business and comply with the requirements of the **General Data Protection Regulations (GDPR)** and Data Protection Act 2018.

1.2. The RAD Information Management Policy and Procedures is part of the RAD's overall Information Strategy.

1.3. The RAD Information Management procedures adopt and comply with the data protection principles as set out in data protection legislation which are that personal information shall be:

1. processed[1] lawfully and fairly[2] and in a transparent manner and where it is clear to individuals what the RAD is doing with their personal information (see Appendix 1, 3 and 5);

2. collected for specified, explicit and legitimate purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes (see Appendix 1 and 3). Further processing for archival historical research would be considered compatible with the initial purpose.

3. adequate, relevant and limited to what is necessary in relation to the purpose or purposes for which it is processed (see Appendix 1);

4. accurate and, where necessary, kept up to date and every step is taken to ensure that personal data that is inaccurate is erased or rectified without delay, having regard to its purpose; (see Appendix 7 and 8);

5. kept in a form which permits identification of individuals for no longer than is necessary for the purpose(s) that the information is processed, personal data for the purposes of archiving for historical research or statistical research will occur subject to the implementation of appropriate technical and organisational measures. (See Appendix 7);

6. 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 (see Appendix 2 and 6);

All employees who process or use personal and special (formerly sensitive) information on behalf of the RAD must ensure that they follow these principles at all times. The RAD and/or individuals could be liable for prosecution and monetary fines for unlawful processing of information.

[1] "Processed" refers to collecting, using, disclosing, retaining or disposing of personal data

[2] "fairly" refers to being open and transparent

1.4. In addition to the above principles the RAD and its employees must also comply with the additional responsibility to demonstrate compliance with the principles, known as the "Accountability Principle". This involves documenting the decisions the RAD takes about privacy in the following ways:

1. Information Audit
2. Processing activity
3. Privacy by design as outlined in the Privacy by Design Policy
4. Impact Assessments as outlined in the Impact Assessment Policy and template
5. Retention Schedule
6. Incident and Breach Reports.

1.5. The RAD sets out the arrangements for information management governance and compliance with the Accountability Principle in its published Accountability Statement.

1.6. In order to ensure that the data protection principles are followed, the RAD has developed this Information Management Policy and Procedures.

2. Scope

2.1. This policy and procedures will operate in all of the RAD's national offices both in the UK and internationally and applies to all employees. The policy is based on EU and UK legislation, but it is expected that all RAD national offices will comply with the policy's main principles and maintain equivalent standards.

2.2. This policy and procedures applies to all personal information which is collected, processed stored and shared about individuals or data subjects.

2.3. It is a condition of employment or engagement that employees abide by the rules, regulations and policies made by the RAD from time to time and which is referred to in the Employee Handbook or Terms and Conditions (freelance workers). Therefore any failure to comply with the Information Management Policy and procedures will be treated as a disciplinary matter and dealt with in accordance with the appropriate RAD's Disciplinary Procedure, which could lead to dismissal.

3. Aims & Objectives

3.1. The aims and objectives of this policy are to:

1. protect the rights of individuals by ensuring that all personal and special information held is used fairly, appropriately and lawfully.
2. minimise the risks to individuals
3. ensure that individuals' right to be informed, right of access, right to rectification, right to erasure, right to restrict processing, right to data portability, right to object and the rights related to automated decision making are available.
4. ensure that all collection, processing, storage and sharing of personal information by the RAD complies with data protection principles.
5. maintain the confidence of individuals by transparency and demonstrating our compliance with legislation.
6. enable RAD risk management of reputational damage and financial penalty.

4. Responsibilities

4.1. The Director of Finance and Operations is the **Senior Information Risk Officer** for both the Royal Academy of Dance and Royal Academy of Dance Enterprises Ltd (RADE) responsible for:

1. fair and legal processing of information via the Information Management Committee.
2. ensuring there are steps being taken in the management of the risks as identified above and in the Academy's Corporate Risk Register.

4.2. There is an **Information Management Committee** which reports to the Executive Board and which meets on a monthly basis to agree best practice to ensure appropriate policies and procedures are in place, that this policy's aims and objectives are achieved, appropriate training provided and data incidents and breaches managed, notified and monitored. The Committee meets on a regular basis with Information Champions (see Information Management Committee terms of reference for further information).

4.3. **Information Asset Owners** are identified and are responsible for the confidentiality, integrity and availability of information maintained by the employees handling the information on a day to day basis in their department.

4.4. Each Department has an **Information Management Champion** who is responsible for providing support to colleagues, promoting data protection awareness, knowledge sharing and implementing data protection procedures.

4.5. **Heads of Departments and Managers** are responsible for ensuring that they have read and understood and follow all relevant policies and procedures related to Information Management and for ensuring that their direct reports understand the same. They are also responsible for ensuring that their direct reports participate in all training provided.

4.6. Those employees who are responsible for collecting, processing, storing and sharing information about individuals must comply with GDPR, the Data Protection Act 2018 Act, this Information Management Policy and Procedures and all other related policies and procedures. They are also responsible for ensuring that they participate in all training provided.

5. Publication & implementation

5.1. The Information Management Policy & Procedures is given to all new employees at Induction and forms part of their initial briefing. The document is available to all employees via SelectHR and all employees will be alerted to revisions.

5.2. The Information Management Policy & Procedures is also available on the RAD website for the general public, employees, freelance workers, students and customers.

6. Training

6.1. In addition to induction, RAD employees are given training in data protection procedures relevant to their role on a biennial basis (or more frequently if legislative or other changes require).

6.2. Information Management Committee members and Information Management Champions are also given regular training on their responsibilities.

7. Policy Ownership & Review

7.1. This policy is owned by the RAD Senior Information Risk Officer who delegates to the Information Management Committee. The RAD is registered with the Information Commissioner in the UK for the processing of personal data. The RAD's current registration numbers (prior to GDPR) are Z5872158 (Royal Academy of Dance) and Z4792277 (Royal Academy of Dance Enterprises Ltd).

7.2. The effectiveness of this policy is the responsibility of the Information Management Committee (see Information Management Committee terms of reference for further information).

7.3. The Information Management Policy & Procedures will be reviewed on an annual basis (or more frequently if legislative or other changes require) by the Information Management Committee for approval by the Executive Board and ratification by the Board of Trustees.

8. Authority & signature

_____

Chairman
On behalf of the Board of Trustees

Revised January 2017, March 2018,
First approved 11 December 2014

Related Documents
Privacy Notice
Information Management Strategy (to be published)
Records Management Policy & Procedures (to be published)
Accountability Statement (to be published)
Privacy by Design Policy (to be published)
Privacy Impact Assessment Policy and template (to be published)
Information Security Policy (to be published)
CCTV Policy

Appendices

A brief summary of the procedures which support this policy is set out in the following appendices:

Appendix 1 Procedure for Privacy Notices

Appendix 2 Procedure for Security of Personal Information

Appendix 3 Procedure for Information Sharing

Appendix 4 Procedure for Individuals Right to Access Personal Information

Appendix 5 Procedure for Authorised Publication or Disclosure of Information

Appendix 6 Procedure for Information Security Incidents and Breaches

Appendix 7 Procedure for Records Retention and Disposal

Appendix 8 Procedure for Erasure, Objection and Restriction of processing

Appendix 9 Glossary of Terms

Full procedure documents are available at www.rad.org.uk and SelectHR document store.

Appendix 1: Procedure for Privacy Notices

The RAD Information Management procedures adopt and comply with the data protection principles as set out in data protection legislation as outlined in 1.3 of this policy.

1. The Procedure for Privacy Notices relates to the data protection principles 1, 2, 3 4 and 5

2. In most cases information collected by the RAD will be obtained directly from individuals often online, sometimes via application / entry forms and occasionally over the telephone or in person. As required by legislation, a Privacy Notice will accompany all requests for personal information.

3. Information on the contents of the Privacy Notice and how it is customised by each department is available in the Procedure for Privacy Notices.

4. The Privacy Notice is made available at all points of contact with individuals, including via the RAD website. The Privacy Notice outlines how information is collected, what type of information is collected, how the information is used and stored, whether third party providers are used, who they are and why. If the lawful basis for the processing is legitimate interest, that will also be disclosed.

5. The RAD also makes the key points of the Privacy Notice clear to those providing personal information in person or over the telephone.

6. Information for individuals on how they can update their information and obtain access to information which is held is also included in the Privacy Notice.

For further information please refer to the full Procedure for Privacy Notices available on SelectHR document store.

Appendix 2: Procedure for Security of Personal Information

The RAD Information Management procedures adopt and comply with the data protection principles as set out in data protection legislation as outlined in 1.3 of this policy.

1. The Procedure for Security of Personal Information relates to data protection Principle 6.

2. All employees responsible for collecting personal information from individuals take personal responsibility for the security of personal data by following RAD standards on secure storage, processing, transfer and disposal of personal data as set out in the Procedure for Security of Personal Information.

3. Individuals have the right to expect that their personal data will be kept and processed securely and that no unauthorised disclosures or transfers will take place to anyone either within the RAD (unless appropriate) or outside the RAD to a third party.

4. Transfers of personal data between departments of the RAD in the UK are authorised where it is for legitimate business need and where it is declared at the point of collection to the "individual" that it is *necessary* for their data to be transferred. Precautions for the safety of data being transferred are available in the Procedure for Security of Personal Information and the separate Information Security Policy.

5. All employees are responsible for ensuring that any personal information that they hold on others is kept, processed, transferred and disposed of securely in accordance with Procedure for Security of Personal Information.

6. Any security of personal information incidents will be reported to the Senior Information Risk Officer, the employee's Line Manager and the Information Management Committee and a documented risk assessment undertaken. Serious incidents will be referred to as breaches and the Procedure for Information Security Incidents will always be followed, including notification to the ICO or other privacy authority, where applicable.

   Please refer to the full Procedure for Security of Personal Information for further information available on SelectHR document store

Appendix 3: Procedure for Information Sharing

The RAD Information Management procedures adopt and comply with the data protection principles as set out in data protection legislation as outlined in 1.3 of this policy.

1. The Procedure for Information Sharing refers to Data Protection Principle 1, 2 and 3

2. Through the nature of the RAD's business in a global market it is necessary for information to be shared with third parties in the UK and within and outside of EEA. In order to comply with the Information Management Policy and Procedures and to ensure the safety of information shared, an Information Sharing Register of Information sharing agreements is maintained. Information on the procedure for the maintenance of the Information Sharing Register is available in the Procedure for Information Sharing.

3. Where it is necessary for information to be shared with a third party (including those inside and outside of EEA) the individual is informed at the point of collection via the Privacy Notice and where applicable permission or consent is obtained, depending on the legal basis for collection.

4. All reasonable steps are taken to ensure that where data is shared outside of the UK that there are adequate standards for the protection of data. Where data is shared outside of the UK and EEA, it will be to the RAD's national offices, the management of which are required to sign up to the standards expected in the RAD's Information Management Policy & Procedures.

5. Where data is shared with other third parties outside of the UK and EEA, it will be with the individuals' agreement and an Information Sharing Agreement will be exchanged. All information sharing agreements will be held on an Information Sharing Register and reviewed at regular intervals.

   Please refer to the full Procedure for Information Sharing available on SelectHR document store

Appendix 4: Procedure for Right to Access Personal Information

The RAD Information Management procedures adopt and comply with the data protection principles as set out in data protection legislation as outlined in 1.3 of this policy.

1. The Procedure for Right to Access Personal Information is related to an individual's right of access as identified in 3.1.2 above and the Right of Access under GDPR and the Data Protection Act 2018.

2. Individuals are entitled to know what information the RAD holds and processes about them and why. They also have the right to gain access to it and know how to keep it up to date.

3. All individuals have a right under data protection legislation to access certain personal information being kept about them either on computer or paper based systems (referred to in legislation as "relevant filing systems"). Any person wishing to exercise this right should email ipoquedp@rad.org.uk

4. All subject access requests (known as SARs) will be dealt with in accordance with the Procedure for Right to Access Personal Information.

5. There is no fee for SARs, but the RAD reserves the right to charge a reasonable fee in the event of unfounded, excessive or repetitive requests.

6. The RAD will comply with SAR requests for personal and special information as quickly as possible and will ensure that it is provided within one calendar month, as required by legislation.

   Please refer to the full Procedure for Right to Access Personal Information available on SelectHR document store

Appendix 5: Procedure for Authorised Publication or Disclosure of Information

The RAD Information Management procedures adopt and comply with the data protection principles as set out in data protection legislation as outlined in 1.3 of this policy.

1. The Procedure for Authorised Publication or Disclosure of Information is related to Data Protection Principle 1 and 2.

2. Whilst the majority of personal information held by the RAD is processed for internal administrative purposes and is never disclosed, some categories of information in some circumstances are authorised for disclosure or publication.

3. The names, images and biographies of Trustees and Directors of the RAD will be published in RAD publications and on RAD websites for marketing purposes and so as to comply with legal requirements.

4. Names of Regional and National staff are also published in RAD publications and on RAD websites to allow the business to function.

5. Biographical details of some employees may be published with the employee's consent for marketing purposes of specific events.

6. Personal information may also be published for marketing purposes in the form of case studies, including images and videos for marketing purposes, but only with the expressed consent of the individual or the consent of a parent or guardian for someone aged 16 and under (see Social Media and Digital Communications Policy)

7. Requests for the disclosure of personal information from the police or other organisation with a crime prevention or law enforcement function, will be fulfilled and considered authorised, provided the authenticity of the person making the request is established, the personal information is being requested to prevent or detect a crime or to catch or prosecute an offender and the risk of not releasing the information would be to seriously impede crime prevention or detection.

8. Employees responsible for personal information collection are made aware by their line managers of the purpose for which the data is processed and the legitimate persons (internally) or organisations (externally) to who it can either in whole or in part be disclosed. Employees must not disclose to any unauthorised third party. Unauthorised disclosure will usually be a disciplinary matter and will be dealt with in accordance with the Disciplinary procedure. Disciplinary action up to and including summary dismissal can be taken.

   Please refer to the full Procedure for Authorised Publication or Disclosure of information available on SelectHR document store

Appendix 6: Procedure for Information Security Incidents and Breaches

The RAD Information Management procedures adopt and comply with the data protection principles as set out in data protection legislation as outlined in 1.3 of this policy.

1. The Procedure for Information Security Incidents and Breaches is related to Data Protection Principle 6.

2. The RAD has security measures in place to prevent incidents and breaches of information security, but in the event of either happening the Procedure for Information Security Incidents will be followed.

3. An Information Security Incident and/or Breach could include:

    a. Loss or theft of RAD personal or special (sensitive) information
    b. Unauthorised alteration or destruction of RAD personal or special information
    c. Loss or theft of information on an RAD computer, device or other equipment
    d. Unauthorised disclosure or of access to personal or sensitive information
    e. Unauthorised use through inappropriate access controls
    f. Equipment failure or human error
    g. Unforeseen circumstances (such as fire, flood or earthquake), anywhere in the world where data is collated and stored on local servers
    h. Loss of availability of personal information
    i. A cyber-attack / hackers
    j. Information obtained from an employee or the RAD by deception.

4. The RAD's Procedure for Information Security Incidents is based on the principles of containment and recovery, assessment of ongoing risk, notification of the breach (where applicable) and evaluation and response.

5. An incident is referred to as a breach where after consideration of the particular case it is considered to be a breach which should be reported to the Information Commissioners Office (ICO) or other equivalent national privacy authority. This will take place when a risk assessment has revealed it is appropriate and the report will be submitted within 72 hours. The Procedure for Information Security Incidents has an **Information Security Incident Report form and Risk Assessment template** and **an Information Breach Notification Report form** template for cases that need to be reported to the ICO or other authority. An **Incident Breach Matrix** (a risk assessment) is also available. All of these resources are available as appendices to the Procedure.

6. Individuals whose personal information has been exposed to risk will also be informed when it is necessary without undue delay.

    Please refer to the full Procedure for Information Security Breaches available on SelectHR document store

Appendix 7: Procedure for Records Retention and Disposal

The RAD Information Management procedures adopt and comply with the data protection principles as set out in data protection legislation as outlined in 1.3 of this policy.

1. The Procedure for Records Retention and Disposal is related to Data Protection Principle 4 and 5

2. The procedure is initially focused on the management of personal and special information with the intention of including all other information types in the future.

3. The procedure ensures that we comply with the principle of keeping information for no longer than is necessary for business purposes and outlines retention rules.

4. Where information is kept for archival purposes or historical research purposes it is subject to appropriate technical and organisational measures and is kept in the Royal Academy of Dance Archive and Special Collection and information about researchers' access to it is available from the Archive and Records manager. The Procedure for Retention and Disposal contains guidance on how to identify records with value for permanent preservation and includes reference to the RAD Archive Collection Policy.

5. The procedure includes all personal and special information which is collected, processed, stored and shared about individuals. This includes records created and received on behalf of the RAD, hard copy and electronic records, including information held on the RAD network, databases, emails, photographs and /or filmed footage (on any medium). (Please also refer to the Visual Media Policy).

6. The procedure supports the disposal of information which has no continuing business, legal or historical significance

7. All records holding personal and special information are kept in accordance with the RAD's Retention Schedule which is an internal operating tool made available to all employees.

8. The procedure contains step by step guidance to assist with the development and implementation of the retention and disposal principles.

Please refer to the full Procedure for Records Retention and Disposal available on SelectHR document store

Appendix 8: Procedure for Right to Erasure, Right to Objection and Right to Restrict processing

The RAD Information Management procedures adopt and comply with the data protection principles as set out in data protection legislation as outlined in 1.3 of this policy.

1. The Procedure for Erasure, Objection and Restriction of Processing is related to individual's rights as identified in 3.1.2 above and the Right to Erasure, Right to Object and Right to Restrict Processing as identified in GDPR and the Data Protection Act 2018.

2. Individuals wishing to exercise these rights are able to through any RAD contact point, but it is recommended that individuals email their request to ipoguedp@rad.org.uk in order for requests to be handled promptly and efficiently.

3. The Procedure for Right to Erasure, Right to Object and Right to Restrict Processing outlines the details of the specific rights, including the circumstances where the rights can be exercised and the procedure that Asset owners should follow when requests are received.

4. The RAD ensures that it has the technical and organisation measures in place to handle erasure, objection and restriction of processing

5. The right of erasure or to be forgotten is a right in specific circumstances as outlined in the procedure. The right of erasure for information supplied by children is very specific.

6. An individual's right to object is for processing based on legitimate interests, ie where they do not agree with the legitimate interest being used. It also applies in the case of direct marketing.

7. An individual's right to restrict processing is often for a temporary period of time in specific circumstances outlined in the Procedure.

Please refer to the full Procedure for Right to Erasure, Right to Object and Right to Restrict Processing available on SelectHR document store

Appendix 9

Glossary of Terms

A glossary of terms used in the Information Management Policy and Procedures and associated policies is available here

Glossary of Terms

Term	Definition
Access	Refers to any mechanisms by which individuals gain access to information. Access can be legitimate or unauthorised.
Accountability Accountability principle Accountability statement	Demonstration of the steps taken and the documentation maintained to comply with the Data Protection principles with explicit responsibilities.
Archive	A store for records which is not part of the daily accessible set. It tends to be offsite, and is generally slower to access, requiring different permissions and request processes. Will generally be subject to RM procedures including retention & disposal.
Asset	See Information Asset
Breach Incident Information Security Incident	A serious security incident is a breach that happens which allows someone (or many people) to see/use/access/share personal information to which they are not allowed or authorised (see incident) A breach is considered serious enough (following a risk assessment) to be reported to the ICO (see ICO) or relevant Privacy Authority (see Privacy Authority)/
Computer software	Computer software is the collection of computer programmes used to process information,

Confidential Confidentiality	Information which requires protection from unauthorised disclosure or intelligible interception (see below for definition).
Cookie	A small piece of information stored on your computer by the owner of any website you visit. This serves a number of purposes, including recognising you later on when you visit again, and for maintaining usage statistics. Use of Cookies is controlled by updates to the interpretation of the DPA by the Commissioner.
Data Controller Responsible Person	The person or body recorded in the Register of Data Controllers held by the ICO. Usually a body for a company. RAD has two: • The Charity arm • The Enterprise arm The DC decides how information is to be used and how it is to be looked after.
Data Processor *(this refers to the legal definition of Data Processors NOT RAD exams staff)*	The person or body which processes data on behalf of the DC, where this is not done inside the organisation the DC represents.
Information Sharing (Data Sharing) Information Sharing Register Information Sharing Agreement	The process of allowing access to your information by a 3rd party. This should be controlled with written Agreements and recorded in a Register.
Data Subject	An individual who is the subject of personal data
Disposal Destruction	Disposal/destruction are terms used to determine the action to be taken when the record reaches the end date defined in the retention criteria See Retention
DPA Data Protection Act (1998) Data Protection Act (2018)	Data Protection Act Current / old version 1998 New version 2018 (as a result of GDPR) – see "GDPR)
Erasure	Individuals have the right to request erasure of their personal information in specific circumstances (see "forgotten)

Forgotten	Right to Erasure is sometimes referred to as right to be forgotten (see "erasure).
FOI Freedom of Information *(the RAD is not legally required to comply with the FOI)*	Freedom of Information allows citizens access to all the other information held by a public body other than their personal information (see SAR).
General Data Protection Regulation (GDPR)	New data protection legislation applicable in the EU and UK and organisations outside of the EU and UK who offer goods and services in the EU and UK.
Heritage Archive	A special store for records which have a long term historical value. May have different criteria for protection and access. Will generally not be subject to retention and disposal requirements.
Incident	An incident occurs when someone (or many people) are able to see/use/access/share personal information to which they are not allowed or authorised (see breach)
Incident Breach Matrix	A risk assessment matrix to use when assessing an information security incident to determine whether it is an incident or breach. (see "incident" and "breach"
Information	Includes data stored on computers, transmitted across computer networks, printed, written, sent by post / fax or stored on removable devices.
Information Asset Information Asset Register Information Asset Owner	A body of information (including computer software and hardware) defined and managed as a single unit so it can be understood, shared, protected and used effectively. A tool to assist with the management of the information assets and the risks to them The individual responsible for ensuring that the risks to, and the opportunities for the asset are monitored. This is not necessarily the creator or the primary user of the asset, but they must understand its value.
ICO Information Commissioner	Information Commissioner's Office (UK) The Commissioner is responsible for ensuring compliance with the Act. See "Privacy Authority".

IG Information Governance	Information Governance is the management structure created to control quality and performance in the management of information, including recording, maintaining, referencing and using information in RAD. Information here is a wide term, and would include all your computer records, paper files, photos, historical records, external archives, and anything else of this nature
IM Information Management	Information Management is the overall collection of arrangements made through Governance and Records Management to look after your information and make available for staff to use safely.
Information Security Incident Report form	The form to complete when an information security incident or breach occurs. The form assists in recording the full extent of the incident, whether it is a breach and whether or not the ICO or other privacy authority and/or the individual(s) should be notified.
Information Breach Notification Report form	The form to complete when it is identified that an incident is a breach and needs to be reported to the ICO (or other privacy authority).
Integrity	Involves safeguarding the accuracy, completeness and consistency of information and computer software.
Intelligible Interception	Intelligible interception is interception of information in such a way that it is readable. Encryption of data might be used to prevent intelligible interception
Object	Individuals have the right to object to their personal information being processed, particularly in direct marketing, but also in other specific circumstances.
Personal Data or Information	Any set of information (manual or electronic) which, together with other information held by the Data Controller, can identify a living person, which may include: • Name • Address • Bank details • Images or pictures • IP address • information regarding the web pages accessed and when. Credit / debit card information

	(The above is a non-exhaustive list of data)
Policy	The top-level description of how you want to behave or perform in a particular matter (e.g. computer security)
Privacy Authority	An authority responsible for data protection and privacy outside of the UK. See "Information Commissioners Officer" and "ICO"
Privacy by Design	Privacy by design is an approach to projects which promotes privacy and data compliance from the start. The approach assists organisations to ensure that privacy and data protection is a key consideration at the start and throughout the life cycle of a project.
Privacy Impact Assessments (PIAs)	Privacy Impact Assessments are a tool which identifies and reduces privacy risks and helps design more efficient and effective processes for handling personal data.
Privacy Notice	The Notice made available to data subjects which explains why we need to have and hold their personal information, what we intend to do with it, and how you will look after it.
Procedure	The detail about how we expect our Policy to be acknowledged and put into effect.
Record Record Series	A record can be defined as recorded information, in any format, which is created or received by RAD or individual members of staff and provides evidence of RAD activities and decisions. A 'record series' is a group of related records which are normally used and filed as a unit. Examples might include minutes from meetings, application forms, annual reports or contracts. Records need to be authentic, reliable, have integrity (be complete or unaltered, except under controlled conditions) and be useable. Records therefore need to be subject to controls that ensure these features are maintained (see IG).
Records Lifecycle	Model used by records managers to describe the stages through which a record progresses during its existence. The stages of a record are • creation • current • semi current • disposition (i.e. archive or destruction)
Records management	Records Management is about applying the necessary controls and creating processes to ensure

	that RAD records are authentic, reliable, usable, up to date, complete and/or accurate.
Restrict	Individuals have the right to restrict the processing of their information in specific circumstances.
Retention	Retention is the rule to determine how long a record should be kept for the purpose understood under Principle 1. See Disposal and Destruction
Retention Schedule	A retention schedule lists the records held and how long they will be retained before disposal action. The schedule also lists how records should be disposed of, i.e. whether they should be destroyed, reviewed prior to destruction or sent to archive. See Disposal and Destruction
RM Records Management	Records Management is the way in which you organise information into accessible records. Accessible means easy to store and easy to find again for reference or use. There are other implications in this for things like accuracy and retention. A Record is generally regarded as a set of information about a subject: for example an athlete, member of staff, business contract, event, Policy and so on.
SAR Subject Access Request	The formal Right under Principle 6 which allows data subjects to have a copy of all the information you hold about them.
Security	Refers to mechanisms and procedures designed to ensure that appropriate controls on information access are in place.
Senior Information Risk Officer	The person with overall responsibility for the management of information and data protection processes at the RAD who delegates responsibility to the Information Management Committee.
Special Data / Information	A particular set of special personal data which to be treated with extra care and sensitivity, as defined by legislation: • Race • Ethnic origin • Political opinion • Physical or mental health condition • Sex life or sexual orientation

	• Religion (or similar) belief • Genetics • Biometrics (where used for ID purposes) • Trade union status • Criminal Record (although not defined as Special, is treated in a similar sensitive way requiring extra care).
Structured Un-structured	Structured is organised using keys or indexes (e.g. by date of birth, by surname or by school) Unstructured means it is not organised in a way which makes it easy to find (e.g. a pile of papers)
Transparent Transparency	Providing accessible information to individuals about how personal data is used. (see Privacy Notice).
User name	A unique identifier which is allocated to employees or students and which together with a password is used to identify and authenticate access to a system.
Vital Records	These are records without which RAD could not function or be recreated in the event of a disaster such as fire or flood.