ROYAL ACADEMY OF MUSIC

DATA PROTECTION POLICY

MARCH 2025

Author: Registrar & Director of Student Operations
Version Number: 3.0

MARYLEBONE ROAD, LONDON NW1 5HT
RAM.AC.UK

UNIVERSITY OF LONDON

Continued overleaf

Title	Data Protection Policy
Owner	Registrar & Director of Student Operations
Contributors	Information Governance Group
Version	3.0
Reviewed by	Policy Review Group
Date of Approval	February 2024
Last Reviewed	March 2025
Next Review	March 2027
Where published	Academy website

TABLE OF CONTENTS

1. AIMS

The Royal Academy of Music (the Academy) aims to ensure that all personal data collected about staff, students, guardians, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. LEGISLATION AND GUIDANCE

This policy meets the requirements of the UK GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

3. DEFINITIONS

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include: • Name • Identification number • Location data • Online identifier, such as a username • Contact details It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special category data	Personal data which is more sensitive and so needs more protection, including: • Racial or ethnic origin • Religious or philosophical beliefs • Political opinions • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Physical or mental health or condition • Sexual orientation
Processing	Any activity relating to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject	The identified or identifiable individual whose personal data is being held or processed.
Data controller	The person or organisation who determines the purposes and means for processing personal data.
Data processor	Any person or organisation that processes data on behalf of the data controller but is not employed by them.
Consent	Clear affirmative action establishing a freely given, specific, informed and unambiguous individual of the individual's agreement to their personal data being processed, such as by a written (including electronic) statement.
Legitimate interest	Legitimate interest is one of the six lawful basis for processes personal data. If you are using Legitimate Interest as a basis to process personal data, then a balance test should be conducted to ensure personal right and freedoms are respected.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. THE DATA CONTROLLER

The Academy processes personal data relating to supporters of students, students, staff, governors, visitors and others, and therefore is a data controller. It is a registered data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. SCOPE

This policy applies to all staff employed by the Academy, and to external organisations or individuals working on our behalf.

5.1 SENIOR MANAGEMENT TEAM

The Senior Management Team holds institutional responsibility for compliance with data protection and information governance. The Registrar & Director of Student Operations leads on this within the group and maintains an overview of all data processing activities, DSARs and breaches in order to be able to report regularly to the Governing Body via the Audit Committee.

5.2 GOVERNING BODY

The Governing Body has overall accountability for ensuring that the Academy complies with all relevant data protection obligations. This responsibility is overseen and monitored by the Audit Committee on its behalf.

5.3 DATA PROTECTION OFFICER

The Data Protection Officer (DPO) is responsible for:

- Auditing data protection arrangements.
- Progressing the Data Protection Action Plan.
- Providing guidance and advice to employees in relation to compliance with legislative

requirements.
- Reporting on any breaches of Data Protection legislation.
- Ensuring those handling personal data are aware of their obligations by supporting the development of relevant policy, auditing processing arrangements and providing training to relevant people.

They provide a twice-yearly report of their activities directly to the Audit Committee. Where relevant, they report to the Governing Body via the Senior Management Team providing their advice and recommendations on data protection issues.

The DPO is also the first point of contact for individuals whose data the Academy processes, and for the ICO.

Our DPO is Black Penny Consulting and is contactable via email (dpo@ram.ac.uk). Full details of the DPO's responsibilities are set out in the service description with Black Penny Consulting.

5.4 HEADS OF DEPARTMENTS

The heads of professional services and principal study departments act as the representative of the data controller on a day-to-day basis and have responsibility to ensure their departmental records and data comply with all relevant data protection obligations.

5.5 ALL STAFF

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy.
- Informing the Academy of any changes to their personal data, such as a change of address, via the self-service facility of iTrent.
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
    - If they have any concerns that this policy is not being followed.
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area.
    - If there has been a data breach.
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
    - If they need help with any contracts or sharing personal data with third parties.

6. DATA PROTECTION PRINCIPLES

The UK GDPR is based on data protection principles that the Academy must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner.

- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.

This policy sets out how the Academy aims to comply with these principles.

7.COLLECTING PERSONAL DATA

7.1 LAWFULNESS, FAIRNESS AND TRANSPARENCY

We will only process personal data where we have one of six 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Academy can **fulfil a contract** with the individual, or the individual has asked Academy of Music to take specific steps before entering into a contract.
- The data needs to be processed so that the Academy can **comply with a legal obligation.**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life.
- The data needs to be processed so that the Academy can perform a task **in the public interest,** and carry out its official functions.
- The data needs to be processed for the **legitimate interests** of the Academy or a third party (provided the individual's rights and freedoms are not overridden).
- The individual (or their guardian or carer when appropriate in the case of a student) has freely given clear **consent.**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018. Further information can be found on the ICO's website.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law. This should include the purposes for processing their personal data, the retention periods for that personal data, and who the data will be shared with. Further information on retention can be found in the Academy's *Data Retention Policy*, which employees can access on the portal.

7.2 LIMITATION, MINIMISATION AND ACCURACY

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Academy's Data Retention Policy, which employees can access via the Sharepoint (Intranet) portal.

8. SHARING PERSONAL DATA

We will not normally share personal data with anyone else, but may do so:

- In specific circumstances, and for legal and professional compliance where there may be a need to share information internally and externally, eg, with NHS services without the consent of the data subject. Examples being a person at immediate and serious risk of suicide, the risk of a criminal offence or harm to others.
- Where we need to liaise with other agencies – we will seek consent as necessary before doing this where our suppliers or contractors need data to enable us to provide services to our staff and students - for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud.
- The purposes of statutory reporting ie to the Higher Education Statistics Agency (HESA).
- The apprehension or prosecution of offenders.
- The assessment or collection of tax owed to HMRC.
- In connection with legal proceedings.
- Where the disclosure is required to satisfy our safeguarding obligations.
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. SHARING PERSONAL DATA

9.1 SUBJECT ACCESS REQUESTS

Individuals have a right to make a 'subject access request' (SAR) to gain access to personal information that the Academy holds about them. This may include:

- Confirmation that their personal data is being processed.
- Access to a copy of the data.

- The purposes of the data processing.
- The categories of personal data concerned.
- Who the data has been, or will be, shared with.
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period.
- The source of the data, if not the individual.
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

If staff receive a SAR they must immediately email the DPO at dpo@ram.ac.uk

Where possible, in their e-mail staff should include:
- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

Unless responsibility has been formally delegated to another member of the Senior Management Team, responsibility for fulfilling a SAR lies with the Registrar and Director of Student Operations. The response to the data subject needs to be within 1 month of first receipt of the SAR. Those responsible should follow the procedure outlined in this policy.

It is important to note that third parties (eg solicitors) can submit a SAR on behalf of their clients. In this instance proof of identification and evidence of authorisation is required.

Data subjects have the right to receive personal data, disclosed as a result of a SAR, in a machine-readable format so that data can easily be transferred to another data controller if necessary. Data controllers are not, however, required to transfer manual records to machine readable format to satisfy such requests.

The Information Commissioner's Office guide provides very useful background information and is essential reading for those who have to deal with SARs.

9.2 CHILDREN AND SARS

Personal data about a child belongs to that child, and not the child's guardians or carers. For a guardian or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from guardians or carers of students may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from guardians or carers of students may be granted without the express permission of

the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

9.3 INFORMATION FOR THOSE SUBMITTING SARS

When responding to requests, we:

- May ask the individual to provide two forms of identification.
- May contact the individual via phone to confirm the request was made.
- May ask for additional detail to be submitted in writing.
- Will respond without delay and within one month of receipt of the request.
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary.
- Will provide the information free of charge, in most cases. Where the request is excessive we may charge a reasonable fee for the administrative costs of complying with the request.

We may not disclose information if it:

- Might cause serious harm to the physical or mental health of the student or another individual, as determined by a medical professional.
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Is contained in adoption or parental order records.
- Is given to a court in proceedings concerning the child.

This is not an exhaustive list of exemptions to the release of information - the DPO will advise on specific cases and in relation to specific information.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO and the ability to seek to enforce this right through a judicial remedy. This information should also be provided where a fee or additional information is requested.

9.4 OTHER DATA PROTECTION RIGHTS OF THE INDIVIDUAL

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time.
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances).
- Prevent use of their personal data for direct marketing.
- Challenge processing which has been justified on the basis of public interest or legitimate interests.
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area.

- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress.
- Be notified of a data breach if it is likely to result in a high risk to their rights and freedoms.
- Make a complaint to the ICO.
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. SHARING PERSONAL DATA

Photography and filming may take place in the following situations:

- Academy performances
- Academy events (including, for example, fundraising events, royal visits, graduation and open days)
- Commissioned photography and film shoots for publications such as the prospectus or Diary of Events
- Rehearsals and preparation for events
- Student examinations and assessments
- Onsite CCTV for security and protection purposes

Information to data subjects:

- Students are made aware of, and consent to, photography and filming when they enrol.
- Visiting artists and professors are required to sign a consent/release form in advance of their visit.
- Any photography involving children is classified as special category information under the GDPR meaning that explicit written guardian or carer consent is always required.
- When individuals attend Academy events they are informed in writing (where appropriate/possible) that photography will take place and the intended use of the images.
- A statement is included in publicity material (where appropriate/possible) explaining that photography will be taking place at an event.
- A notice is displayed at the venue (where appropriate/possible) explaining that photography or filming will be taking place.
- Clear signage is in place for any areas covered by CCTV.

Uses of related data:

- Promotional purposes, including use in the Academy's printed materials and on its digital channels.
- Use by selected third parties for the Academy's promotional purposes ('promotional purposes' include but are not limited to marketing, media coverage, fundraising and recruitment).
- Archive and educational purposes.
- Assessment/study purposes of conducting, choral conducting and composition students (where such students will be provided with copies of the recordings on request).

Video footage and/or photographs will be held in perpetuity as part of the Academy's historic archive. CCTV footage is retained for 30 days.

11. DATA PROTECTION BY DESIGN AND DEFAULT

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6).
- Completing data protection impact assessments (DPIAs) where the Academy's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies- please see the Academy's Data Protection Impact Assessment Procedure on SharePoint (Intranet) https://royalacademyofmusic.sharepoint.com/sites/dataprotection.
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the contact details of the Academy's DPO and all information we are required to share about how we use and process their personal data (via our privacy notices).
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

12. DATA SECURITY AND STORAGE OF RECORDS

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data should be kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.
- Where personal information needs to be taken off site, staff must have read and understood the academy's 'Working From Home Policy.' Staff must ensure information is stored securely whilst off site.
- Academy computers, laptops and other electronic devices must be protected by strong

passwords (passwords that are at least eight characters long and contain letters and numbers). Staff and students are reminded to change their passwords at regular intervals and to lock their devices when not in use. It is recommended that staff use different passwords for personal and work devices and accounts.
- Encryption software is being introduced to protect all portable devices and removable media, such as laptops and USB devices.
- To keep information safe when using public Wi-Fi, staff should only login to networks that are password protected and use a VPN where possible. Staff should check that websites contain 'https' (the 's' stands for secure) before logging into any accounts and log out when finished. File sharing should be disabled and Wi-Fi/Bluetooth turned off when not in use.
- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for Academy -owned equipment.

Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

13. DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Academy's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

More information on how to deal with specific types of records can be found in the Academy's Data Retention Policy, which employees can access via the SharePoint (Intranet) portal.

14. PERSONAL DATA BREACHES

The Academy will make all reasonable endeavours to ensure that there are no personal data breaches.

In the event of a suspected data breach, staff must follow the procedure set out in Appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches could include, but are not limited to:
- A non-anonymised dataset being published on the Academy's website which shows sensitive personal data.
- Safeguarding information being made available to an unauthorised person.
- The theft of a laptop containing non-encrypted personal data about students.

15. TRAINING

All staff at the Academy are provided with data protection training as part of their induction

process.

Data protection will also form part of continuing professional development, including mandatory refresher training every two years and updates where changes to legislation, guidance or Academy processes make it necessary.

16. MONITORING ARRANGEMENTS

The DPO is responsible for monitoring and reviewing this policy in collaboration with the Information Governance Group.

This policy will be reviewed and updated if any changes are made to legislation that affect the Academy's practice. Otherwise, this policy will be reviewed **every two years** and shared with the Audit Committee.

17. LINKS WITH OTHER POLICIES AND PROCEDURES

This data protection policy is linked to the following policies, all of which can be found on the portal:

- Privacy Policy (enrolled students)
- Privacy Policy (Junior Academy)
- Privacy Policy (members of the Governing Body [Trustees] and external committee members)
- Privacy Policy (job applicants and employees)
- Privacy Policy (external parties)
- Records Management Policy
- ICT Acceptable Usage Guidelines
- Working From Home Policy
- Data Retention Policy
- Data Protection Impact Assessment (DPIA) Procedure
- Conflict of Interests Policy
- Adult (over 18) Safeguarding Policy
- Under 18s Safeguarding Policy

APPENDIX: PESONAL DATA BREACH PROCEDURE

This procedure is based on guidance on personal data breaches produced by the ICO.

Identifying a Data Breach

A data breach is any action or incident that puts the personal data of any individual at risk. Examples of data breaches include:

- A staff member leaves papers containing information about students' academic performance on a train. The papers were not in a locked case.
- Ransomware locks electronic files containing personal data.
- Sending an email containing personal data to the incorrect recipient.
- A filing cabinet is not emptied before being sold or sent for disposal, and contains historic personnel files.

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify dpo@ram.ac.uk

If certain criteria apply, the breach must be notified to the ICO within 72 hours of it being discovered, and therefore it is important that any breach - however minor - is reported as soon as it is discovered so that immediate action can be taken.

Once notified, the DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

If the breach is determined to be serious, the DPO will alert the relevant senior staff.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary (actions relevant to specific data types are set out at the end of this procedure).

All staff must comply with and assist the DPO in carrying out this operation.

The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen. The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (eg emotional distress), including through:

- Loss of control over their data
- Discrimination

- Identify theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned.

If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

The DPO will document the decision (either way) in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored electronically with restricted access for the DPO and the relevant Head/Principal and Data Protection Champion.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
  - The categories and approximate number of individuals concerned.
  - The categories and approximate number of personal data records concerned.
- The name and contact details of the DPO.
- A description of the likely consequences of the personal data breach.
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO.
- A description of the likely consequences of the personal data breach.
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored electronically with restricted user access for the DPO, and the Data Protection team.

Where a risk to the reputation of the Academy is identified an action plan will be put in place by

the Senior Management Team.

The DPO and Data Protection team will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible, and lessons learnt will be shared with the Information Governance Group.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the Head of IT will ask the ICT department to recall it.
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Academy/staff members laptop containing non-encrypted sensitive personal data being stolen or hacked (student's personal information, written statements)

- If the laptop containing the information is suspected stolen, the staff member responsible for that computer should report this to the DPO and the police.
- If the laptop containing the information has been lost, the staff member responsible for that computer must attempt to locate it or failing that attempt to access the hard drive from an external source (if possible).
- The DPO should be informed as soon as this information is in danger of being shared to unauthorised individuals from the laptop.
- If recall of the laptop is unsuccessful then the DPO must contact the ICO and report the breach of data through the correct procedure.

Ransomware locks electronic files containing personal data

- Whoever identifies this should notify the DPO, and the Head of ICT immediately.

- Backups of the data should be accessed, and action should be taken to ensure that the systems are secured.
- The DPO and the Head of IT will work together to mitigate any initial risks, and notify the ICO where appropriate.