Adagio School of Performing Arts

Data Protection Policy

Approved by:	The Principal
Reviewed by:	Bronwen Patching
Date:	20th of October 2021
Next Review:	Autumn Term 2022

Contents

Policy Statement

It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly. A good rule of thumb here is to ask yourself questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?
- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?
- What would be the consequences of my losing or misdirecting this personal data? Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how handle and record personal information and manage our relationships with people. This is an important part of the School's culture and all its staff and representatives need to be mindful of it.

1.Aims

ASOPA processes certain personal data about its employees and students for a variety of defined purposes, such as to allow us to allow access to computer systems and monitor performance, achievements, and health and safety. In order to protect the privacy of employees and students and to comply with the principles laid out in law, information must be collected and used fairly, stored securely and confidentially, and destroyed when it is no longer needed.

Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. ASOPA aims to ensure that all personal data collected about staff and pupils, parents, visitors and other individuals is collected, stored and processed lawfully in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and 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

ASOPA collects and uses student information under section 537A of the Education Act 1996, and section 83 of the Children Act 1989. We also comply with Article 6(1)(e) and Article 9(2)(b) of the General Data Protection Regulation (GDPR).

This policy meets the requirements of the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018). It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

3. Definitions

Staff: all employees, workers, volunteers and others.

Consent: a freely given, specific, informed and unambiguous indication of a data subject's agreement to the processing of personal data relating to them, given by a clear positive action.

Data Breach: the accidental or unlawful destruction, loss, alteration or unauthorised access, disclosure or acquisition, of personal data.

Data Controller: the person/organisation that determines when, why and how to process personal data.

Data Owners: Directors responsible for key categories of personal data.

Data Sharing Agreement (DSA): a legal agreement or contract outlining data sharing activity and the responsibilities of parties who are sharing data.

Data Subject: a living, identifiable individual about whom we hold personal data. Data subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

General Data Protection Regulation (GDPR): the General Data Protection Regulation (*(EU) 2016/679*).

Personal Data: any information which, either on its own or if combined with other information could uniquely identify a data subject. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion or intention.

Privacy Notices: notices setting out information about the processing of personal data, which must be provided to data subjects when we collect information about them.

Processing or Process: any activity that involves the use of personal data, including obtaining, recording storing, organising, amending, retrieving, using, disclosing, transferring, erasing or destroying it.

Pseudonymisation or Pseudonymised: replacing identifying information with a pseudonym, so that the data subject cannot be identified without the use of information, which is kept separately and securely.

Special Category Data: personal data revealing race or ethnicity, political opinion, religious beliefs, trade union membership, health conditions, sex life, sexual orientation, biometric or genetic data, or criminal offences or convictions.

4. The data controller

ASOPA processes personal data relating to parents, pupils, staff, visitors and others, and therefore is a data controller.

5.Scope

This policy applies to all employees, volunteers, students and customers of ASOPA who process personal data, and covers all personal data we process, regardless of the method of storage or type of data subject. This includes emails, notes and documents containing personal data.

6.Roles and responsibilities

- **Data protection officer**

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

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

The DPO for ASOPA is Bronwen Patching

- **All staff**

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of anychanges to their personal data, such as a change of address
- 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.
- 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

7.Core Principles

ASOPA complies with the following GDPR data protection principles or rules of good information handling.

These principles require that personal information is:

- 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, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and accidental loss, destruction or damage
- Processed in a way that ensures it is appropriately secure
- Not transferred to another country without appropriate safeguards being in place
- Made available for data subjects to exercise certain rights in relation to their personal data

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

8. Collecting Personal Data

ASOPA collects and uses student information under section 537A of the Education Act 1996, and section 83 of the Children Act 1989. ASOPA also comply with Article 6(1)(e) and Article 9(2)(b) of the General Data Protection Regulation (GDPR).

a. Lawfulness, fairness and transparency

ASOPA will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that ASOPA can **fulfil a contract** with the individual, or the individual has asked ASOPA to take specific steps before entering into a contract;
- The data needs to be processed so that ASOPA can **comply with a legal obligation**;
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e. to protect someone's life;
- The data needs to be processed so that ASOPA, as a public authority, can **perform a task in the public interest or exercise its official authority;**
- The data needs to be processed for the **legitimate interests** of ASOPA (where the processing is not for any tasks ASOPA performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden;

- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent.**

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a student) has given **explicit consent;**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment,**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent;
- The data has already been made **manifestly public** by the individual;
- The data needs to be processed for the establishment, exercise or defence of **legal claims;**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation;
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law.
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law;
- The data needs to be processed for **archiving purposes**,

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent;**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent;
- The data has already been made **manifestly public** by the individual;
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights;**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

b. Limitation, minimisation and accuracy

ASOPA 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.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

9. Sharing personal data

ASOPA will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a student or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- 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 contract with the supplier or contractor 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

ASOPA will also share personal data with law enforcement and government bodies where we are legally required to do so.

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 internationally, we will do so in accordance with data protection law.

10. Subject access requests and other rights of individuals

Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that ASOPA holds about them. This includes:

- 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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- 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
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but ASOPA may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

To make a 'subject access request', contact ASOPA admin@adagioschool.co.uk **or phone on 01277 224345**

If staff receive a subject access request in any form, they must immediately forward it to the DPO

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification;
- May contact the individual via phone to confirm the request was made;
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant);
- Will provide the information free of charge;
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month and explain why the extension is necessary.

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the student or another individual;
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests;
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it;

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

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 (in certain circumstances)

- Prevent use of their personal data for direct marketing
- Object to processing, which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- 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.

11. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 working days of receipt of a written request.

If the request is for a copy of the educational record, ASOPA may charge a fee to cover the cost of supplying it.

This right applies as long as the student concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the student or another individual, or if it would mean releasing exam marks before they are officially announced.

12. CCTV

ASOPA use CCTV in various locations around the builiding to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to admin@adagiocollege.co.uk

13. Photographs and videos

As part of our ASOPA activities, we may take photographs and record images of individuals within ASOPA.

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at ASOPA events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other students are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where ASOPA takes photographs and videos, uses may include:

- Within college on notice boards and in ASOPA brochures, newsletters, etc.
- Outside of ASOPA by external agencies such as the college photographer, newspapers, campaigns
- Online on the ASOPA website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the student, to ensure they cannot be identified.

Please refer to our Safeguarding and Social Media policies for more information on our use of photographs and videos.

14. Data protection by design and default

ASOPA 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 where ASOPA's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- 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 name and contact details of ASOPA and 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, type of data subject, how and why we are using the data, any third-party recipients.

15. Storage Limitation

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

Personal Data will not be kept for longer than is necessary for the purposes for which the data is processed, including for the purpose of satisfying any legal, accounting or reporting requirements.

ASOPA will maintain a central Data Retention Procedure and Schedule, and each department or business area is required to maintain a local Retention Schedule, which outlines the time for which personal data may be stored. Staff members must ensure that they delete personal data, taking all reasonable steps to destroy or erase from all storage systems, including paper and electronic copies. This includes erasure of emails containing personal data and requiring third parties to delete such data where applicable.

16. 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 ASOPA's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

ASOPA will make all reasonable endeavors to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in an educational context may include, but are not limited to:

- Safeguarding information being made available to an unauthorized person
- The theft of a school laptop containing non-encrypted personal data about students

18. Training

All staff are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the ASOPA's processes make it necessary.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed every **2 years.**

20. Links with other policies

This data protection policy is linked to our:

- Safeguarding Policy
- E-Safety Policy
- Social Media policy

Appendix 1: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- 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
- 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)
- 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 (e.g. 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
- 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.
- 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:
    - A description, in clear and plain language, of the nature of the personal data breach
    - 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

  As above, any decision on whether to contact individuals will be documented by the DPO.
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts relating to the breach
    - 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 securely on the icloud system.
- The DPO and Administration 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

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.

For example:

Special category data (sensitive information) being disclosed via email (including safeguarding records)

- If special category data 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 DPO will attempt to retrieve 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 anyway
- 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