ART ACADEMY
LONDON

Data Protection Policy

1. Introduction

The Art Academy processes the personal data of living individuals such as its staff, students, contractors and customers. This processing is regulated by the Data Protection Act 2018 (DPA 2018) and General Data Protection Regulations (GDPR). The UK's regulator for the DPA and GDPR is the Information Commissioner's Office (ICO). The Academy is registered as a Data Controller with the ICO and is responsible for compliance with the GDPR and DPA.

1.1Key Definitions

This DPA and GDPR contain a number of key definitions which are referenced in this policy:

Personal data is any information from which an individual can be identified, either directly (from that data alone) or indirectly (if someone could work out who the person referred to is from the data or by matching against other data). Examples of personal data include names, student ID numbers and IP addresses. Further guidance on determining what is personal data is available from the Information Commissioner's website.

'Sensitive Personal Data' means information about an individual's ethnicity, political opinions, their religious beliefs or other beliefs of a similar nature, membership of a trade union, disability, sexual orientation, the commission or alleged commission by them of any criminal offence, or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings of the sentence of any court in such proceedings.

Under the GDPR, the term 'sensitive personal data' will be replaced by the definition '**special category data'** which means any personal data information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and their genetic or biometric data.

Processing; means any operations or set of operations which is performed on personal data whether or not by automated means such as collection, use, disclosure or storage of personal data etc.

'Data Controller' means the organisation which, either alone or jointly with another organisation, determines the manner and purpose of the processing of personal data. The Data Controller is responsible for compliance with the DPA and GDPR.

'Data Processor' means an organisation (such as a contractor) which processes personal data on behalf of a Data Controller.

'Personal Data Breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

1.2 Purpose and Objectives

This policy sets out the Academy's commitment to comply with the Data Protection Act 2018 (DPA 2018) and General Data Protection Regulations (GDPR).

The DPA and GDPR are both centred on key data protection principles:

- Personal data shall be processed fairly and lawfully
- It shall be obtained for specified purposes
- It shall be adequate, relevant and not excessive
- It shall be accurate and up-to-date
- It shall not be kept longer than necessary
- It shall be processed in accordance with the rights of the data subject
- Measures shall be taken to protect processing, and to prevent loss and damage

- It shall not be transferred outside the European Union unless there is an adequate level of protection in that country

The Information Commissioner's Office (ICO) is the regulator for data protection matters and can issue fines for breaches of the law. From 25 May 2018, the maximum fine for breaching the GDPR will be 20 million euros or 4% of the Academy's annual turnover (whichever is highest).

1.3 Scope and Status

This policy applies to all Academy staff, students and others who use or process any personal data. This policy applies regardless of where personal data is held and or the equipment used if the processing is for the Academy's purposes. Further, the policy applies to all personal data, sensitive personal data or special category data held in any form whether manual paper records or electronic records.

2. Roles and Responsibilities

The Board of Trustees: The Board of Trustees is responsible for approval of the Policy.

The Executive Team: The Executive team, and primarily the Director of Operations and Finance, is responsible for strategic level implementation of the policy, oversight of compliance with the policy and reporting identified risks to the Board.

Data Protection Officer: The Academy's Data Protection Officer (DPO) is primarily responsible for advising on and assessing the Academy's compliance with the DPA and GDPR and making recommendations to improve practice in this area. Further, the DPO acts as the Academy's primary point of contact for DPA and GDPR matters.

All staff: All staff, including permanent staff, fixed term contractors and temporary workers must comply with this Policy, the DPA and GDPR whenever processing personal data held by the Academy or on behalf of the Academy.

All Students: All students are responsible for compliance with the rules and policies made by the Academy. Students must comply with this policy where collecting and processing personal data as part of their course, studies or research.

Contractors and Consultants: Third parties such as consultants, contractors or agents, undertaking work on behalf of the Academy involving personal data, must adhere to the Academy's Data Protection Policy and comply with the DPA and GDPR. Provision will be made in contracts with external providers to ensure compliance with this Policy, the DPA and GDPR.

3. Compliance with the DPA and GDPR

3.1Awareness & Capability

The Academy will implement, and monitor completion of, mandatory Data Protection training for all staff and tutors. The content of that training will be reviewed annually and the relevant parties receive updates and refreshers when appropriate.

3.2 Privacy By Design

The Academy will implement a Privacy By Design Approach to processing personal data through integrating Privacy Impact Assessments into business processes and projects. 'Privacy by Design' requires that organisations consider privacy issues at the outset of projects, processes or systems which involve the processing of personal data and identify measures to mitigate risks to individuals' privacy rights.

Privacy Impact Assessments (PIA) are an integral part of taking a Privacy by Design approach to processing of personal data.

3.3 Record Keeping & Retention

The Academy will maintain a Records Retention and Disposal Schedule setting the periods for which records containing personal data are to be retained.

3.4 External Contractors and International Transfers

The Academy will enter into legally binding contracts with external bodies where those bodies are engaged to process personal data on our behalf. The Academy will implement adequacy arrangements where transferring any personal data outside of the European Union.

3.5 Other Third Party Access

The Academy will only disclose personal data to third parties such as the police, central government and other education institutions where there is a lawful basis for doing so and appropriate arrangements are in place with those parties.

3.5.1 Sharing with Regulatory bodies, Partner Organisations, Contractors and Suppliers

A written contract will always be used where we are required to disclose personal data to an organisation or instruct another organisation to process personal data on our behalf (either personal data which the Academy discloses or where the Academy instructs another organisation to collect personal data on our behalf). That contract will include appropriate measures to protect the security of the personal data in question.

In regards to students, this will include the disclosure of personal data to external organisations which is required for the operation and administration of higher education provision. This may include the following organisations:

- Student sponsors and any relevant funding body;
- the Home Office, UK Visas and Immigration (or any body that replaces it), Higher Education Statistics Agency and professional and regulatory bodies;
- validating/ accrediting bodies;
- debt collection agents, third party service providers and external research and survey organisations;

3.5.2 One-Off Disclosures

In some cases, we might be asked to make a one-off disclosure of someone's personal data to another party. Before we do so, we will consider whether we have a lawful basis for disclosing (such as consent).

Common requests of this nature:

- Requests for personal data from the police should be referred to the Academic Quality and Programme Manager (students and tutors) or the Operations Manager (staff)
- Requests from local authorities for the purpose of assessing council tax exemption of students will be answered. The request must confirm why the information is required, be in writing and be from an official local authority email address. Only basic details such as name, address and course dates will be made available in response.
- Employers and prospective employers and other educational institutions (for reference purposes).
- We don't release students' personal data to parents/next of kin unless expressed permission has been given by the student and the parent/next of kin are identified using security protocol.

3.6 Internal Sharing

The Academy will seek to ensure that personal data is only shared across different teams or departments where those areas have a business need for accessing that data.

4. Data Subjects Rights

The Academy will comply with requests from an individual to exercise their rights under the DPA, and from 25 May 2018, the GDPR. All individuals have the right to be informed what information the Academy holds about them and to request copies of that information. This is known as a Subject Access Request. Any individual wishing to submit a Subject Access Request should follow the instructions accessible here.

Under the DPA and GDPR, individuals also have the following rights in relation to their personal data:

- A right of access to a copy of the information comprised in their personal data
- The right to request their personal data is rectified if inaccurate
- The right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed.
- The right to request that the processing of their personal data is restricted
- The right of portability in relation to their personal data
- The right to object to processing that is likely to cause or is causing damage or distress.
- The right to prevent processing for direct marketing
- The right to object to processing which involves automated decision making or profiling.
- The right to claim compensation for damages caused by a breach of the Act

Individuals who wish to exercise the above rights should contact the Operations Manager. Individuals should submit their request in writing and specify exactly what personal data and/or processing they are referring to and which right they wish to exercise. If you are seeking access to your personal data (i.e. making a 'Subject Access Request') then you may find it helpful to complete the Academy's Access to Information Form (Data Protection).

All staff are responsible for cooperating with Operations Manager to ensure that the Academy can comply with an individual's request under the DPA and GDPR within the statutory timescale: there is a strict calendar timescale for responding to requests for access to personal data. From 25 May 2018, this deadline will be reduced from 40 to 30 days.

From 25 May 2018 institutions are no longer allowed to charge a fee for meeting requests for information, in accordance with the GDPR.

5. Own Personal Data

All staff and students are responsible for checking that information they provide to the Academy in connection with their employment or studies is accurate and up to date. Any changes to personal data provided (e.g. change of address) must be promptly notified, in writing, to the Academic Quality and Admissions Coordinator (Students and tutors) or The Operations Manager (staff). The Academy cannot be held responsible for errors unless the member of staff or students has properly informed the Academy about them.

6. Personal Data Breaches

The Academy will respond promptly to any identified personal data breaches and thoroughly investigate those incidents to ascertain whether:

- The breach should or must be reported to the ICO.
- Data subjects should or must be made aware of the breach; and
- It is necessary to amend processes or introduce new measures to mitigate against any further breaches.

Any staff member who knows or suspect an actual or potential personal data breach has occurred must immediately notify the Data Protection Officer. All staff are responsible for fully engaging and cooperating with the Data Protection Officer in relation to their investigation of a personal data breach.

6.1 Definition of a Personal Data Breach

A personal data breach means a breach of security leading to the **destruction, loss, alteration, unauthorised disclosure of, or access to, personal data**.

Data means information in any format, eg, papers, records, emails, faxes etc. The definition of personal data can be complex and, in the event of a breach, it is safest to assume any information about a living individual is personal data and may include;

- Factual information about an individual such as name, student identification number, date of birth, address, bank account details.

- Sensitive information such as information about mental and physical health, sexual life, criminal records and activities, ethnicity and religion.
- Opinions expressed about an individual for example in staff or student appraisals or email exchanges.

Examples of personal data breaches include:

- Leaving paper records on a train.
- Email personal data to the wrong person.
- Deleting personal data when it is still needed.
- Losing a memory stick containing personal data.

7. Compliance

Compliance with this Policy, the DPA and from May 2018, the GDPR is the responsibility of all members of staff and students. Staff and tutors must comply with the rules and procedures made by the Academy. It is a condition of being a student that all Academy rules and policies are fully complied with. Any breach of the policy by a member of staff or tutor may result in disciplinary action or access to the Academy's facilities being withdrawn.

Serious or deliberate breaches of the DPA can result in a criminal prosecution. Any breach of the GDPR by the Academy may result in a substantial fine or actions imposed upon the Academy by the ICO.

8. Further Information

Questions about the interpretation or operation of this policy should be taken up in the first instance with the Data Protection Officer. Any individual who considers that the Policy has not been followed in respect of personal data about themselves should also raise the matter with the Academy's Data Protection Officer. Further information about the Data Protection Act 2018 and the GDPR can be found on the Information Commissioner's Office (ICO website).

Policies and documents that supplement and reference this document:

Student Handbook
Tutor Handbook
Staff Handbook
Freedom of Information Policy and Publication Scheme
Information Security Procedures
Data Retention Schedules

Version 1	May 2018	Awaiting approval by the Trustees