Document Title: Data Protection Policy
Owner: Company Secretary
Author: Louise Wilkins
Date Approved: 3 March 2025
Approved by: Council upon recommendation of E&I Committee
Cycle for Review: every 3 years
Date for Next Review: March 2028
Location of Publication: AA website and intranet

DATA PROTECTION (GDPR) POLICY

1. Introduction

This Data Protection Policy sets out how the Architectural Association (AA) handles the Personal Data of its students, members, employees, workers, suppliers and other third parties.

This Data Protection Policy applies to all Personal Data processed by the AA regardless of the media on which that data is stored or whether it relates to past or present students, members, employees, workers, suppliers, website users or any other Data Subjects.

This Data Protection Policy applies to all AA employees and workers who must read, understand, and comply with this Policy when processing Personal Data on behalf of AA. Compliance with this Policy is mandatory for all AA staff and consultants, and compliance is supported through training. Related procedures and privacy notices are available on the AA intranet. Any breach of this Data Protection Policy may result in disciplinary action.

2. Scope

Protecting the confidentiality and integrity of Personal Data is a critical responsibility that the AA takes seriously at all times particularly given the risk of harm to individuals, and breach of legal requirements if the Policy is not adhered to.

The Data Protection Officer (DPO) is responsible for overseeing this Data Protection Policy and developing related policies, procedures, and guidance. The DPO is the Company Secretary of the AA, and can be contacted on dataprotection@aaschool.ac.uk.

3. Definitions

The General Data Protection Regulation (GDPR) governs processing of personal data with the following definitions being used:

- **Personal Data:** This refers to any information that relates to an identifiable natural person. Examples include names, addresses, email addresses, and IP addresses.

- **Special Category Data:** This is a subset of personal data that is considered more sensitive and requires additional protection. This is defined in Section 5.

- **Data Subject:** This is the individual whose personal data is being collected and processed.

- **Data Controller:** This is the entity (either a person, company, or organisation) that determines the purposes and means of processing personal data. They decide 'why' and 'how' the data is processed.

- **Data Processor:** This is the entity that processes personal data on behalf of the data controller. They follow the instructions of the data controller and do not own or control the data themselves.

4. Personal data protection principles

The AA, as Data Controller is responsible for and must be able to demonstrate compliance with the following data protection principles: -

- **Lawfulness, Fairness, and Transparency:** Personal data must be processed lawfully, fairly, and in a transparent manner. This means the AA needs a valid legal basis for processing data and must process it in ways that individuals would reasonably expect and be clear and open about how the AA uses their data.

- **Purpose Limitation:** Data should be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This ensures that data is only used for the reasons it was originally collected.

- **Data Minimisation:** Only the minimum amount of data necessary for the intended purpose should be collected and processed. This principle helps reduce the risk of data breaches and ensures that unnecessary data is not collected.

- **Accuracy:** Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that inaccurate data is erased or rectified without delay.

- **Storage Limitation:** Personal data should be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed. Once the data is no longer needed, it should be securely deleted.

- **Integrity and Confidentiality**: Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage. This involves implementing suitable technical and organisational measures

5. Special Category Personal Data

Some types of data require additional protection due to its sensitive nature and such data should only be processed when absolutely necessary. Special Category data is: -

- personal data about racial or ethnic origin;
- personal data about political opinions;
- personal data about religious or philosophical beliefs;
- personal data about trade union membership;
- genetic data;
- biometric data (where used for identification purposes) – this could be data such as fingerprints or retina scans;
- data concerning health;
- data concerning a person’s sex life; and
- data concerning a person’s sexual orientation.

6. Legal basis for processing

- **Consent**: The individual has explicitly given their agreement to the processing of their personal data for the

purpose stated to them.

- **Contract:** Processing the personal data is necessary to fulfill a contract that involves the data subject.

- **Legal Obligation:** Processing personal data is required for legal or regulatory reasons.

- **Vital Interests:** Processing the personal data is necessary to protect an individual at risk of harm

- **Legitimate Interest:** Processing is necessary for the purposes of the legitimate interests pursued by the AA except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. Legitimate interest is the most flexible legal basis and most appropriate to use where minimal privacy impact, the data subject would reasonably expect their personal data to be processed for this reason, and the processing of the data is necessary.

7. When to seek advice from the DPO

Please contact the DPO with any questions about the content of this Data Protection Policy or data privacy obligations. In particular, you must always contact the DPO in the following circumstances:

- if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the AA);
- you are planning a project that will involve the processing of a significant amount of Personal Data;
- you are planning a project that may result in a high risk to the right and freedoms of individuals;
- if you need to rely on Consent and/or need to capture Explicit Consent to process Personal Data;
- if you need to draft a Fair Processing Notice;
- if you are unsure about the retention period for the Personal Data being processed;
- proposal to use automatic decision making or profiling;
- if you are unsure about what security or other measures you need to implement to protect Personal Data;
- if there has been a Personal Data Breach;
- if you are unsure of what basis to transfer Personal Data outside the EEA, or transfer personal data to another country to ensure appropriate safeguards are in place
- if you need any assistance dealing with any rights invoked by a Data Subject;
- whenever you are engaging in a significant new, or change in processing activity which is likely to require a DPIA, or plan to use Personal Data for purposes other than what it was collected for;
- if you need help complying with applicable law when carrying out direct marketing activities; or
- if you need help with any contracts or other areas in relation to sharing Personal Data with third parties.
- proposing to process Special Category Personal Data.

8. Data Subject Rights

Individuals have the following rights regarding their personal data:

- **Right to be Informed**: Individuals have the right to be informed about the collection and use of their personal data.

- **Right of Access:** Individuals have the right to access their personal data and obtain information about how it is being processed.

- **Right to Rectification:** Individuals have the right to have inaccurate personal data rectified or completed if it is incomplete.

- **Right to Erasure**: Individuals have the right to have their personal data erased in certain circumstances.

- **Right to Restrict Processing:** Individuals have the right to request the restriction or suppression of their personal data in certain circumstances.

- **Right to Data Portability:** Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

- **Right to Object:** Individuals have the right to object to the processing of their personal data in certain

circumstances.

- **Rights Related to Automated Decision-Making and Profiling:** Individuals have the right not to be subject to a decision based solely on automated processing, which significantly affects them.

A copy of all data privacy policies and procedures are available on the Key Documents page under Data Privacy on the AA's intranet. LINK

AA staff receiving the request must immediately send onto dataprotection@aaschool.ac.uk and secretary@aaschool.ac.uk who will verify prior to processing the request.

9. Data Security

The AA implements appropriate measures to ensure the security of personal data. This includes:

- **Access Controls**: Limiting access to personal data to authorised staff only.
- **Encryption:** Using encryption to protect personal data during transmission and storage.
- **Regular Audits:** Conducting regular audits to ensure compliance with data protection policies and procedures.
- **Incident Response:** Establishing procedures for responding to data breaches and other security incidents
- **Information Security Policy:** Defining principles and a robust framework for managing information security across the institution, clarifying responsibilities at all levels within the AA. Cultivating a security-aware culture among staff, students, members and authorised users.

10. Reporting a Personal Data Breach

The UK GDPR requires Data Controllers log and, in some instances, to notify certain Personal Data Breaches to the Information Commissioners Office or 'ICO' and, in certain instances, the Data Subject.

The AA has a procedure in place to highlight and take mitigating actions for any suspected Personal Data Breach and to notify Data Subjects, and ICO where we are legally required to do so.

If any AA staff, member, or student knows or suspects that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the IT Team via itsupport@aaschool.ac.uk and Data Protection Officer dataprotection@aaschool.ac.uk. The Data Protection Officer will determine whether the breach meets the notification requirements.

11. Data Protection Officer

The AA has appointed a Data Protection Officer (DPO) who is the Company Secretary of the AA, who is responsible for overseeing data protection strategy and implementation to ensure compliance with UK GDPR requirements. The DPO can be contacted at dataprotection@aaschool.ac.uk

12. Academic Research

Academic research which involves the processing of personal data is subject to the General Data Protection Regulation. Consideration should be given to 'what' and 'why' data is being processed as part of the research project, and the Ethics and Ethical Review Process followed – see Key Documents page on the intranet. LINK

13. Training and Awareness

All AA staff members are required to undergo data protection training to ensure they understand their responsibilities under UK GDPR and the Data Protection Act 2018. Regular updates and refresher training will be provided. Further resources are provided on the staff intranet and on request from the Date Protection Officer.

14. Data Sharing and Transfers

Personal data shall only be shared with third parties when there is a legitimate reason to do so, and appropriate safeguards are in place. Transfers of personal data outside the European Economic Area (EEA) shall be conducted in compliance with UK GDPR requirement and in consultation with the DPO.

15. Data Protection by Design, Data Protection Impact Assessments (DPIAs)

The AA is required to ensure Privacy by Design is built into its processes and outcomes. DPIAs shall be conducted for any new or significantly changed processing activities to identify and mitigate data protection risks. The AA shall follow ICO guidance on conducting DPIAs. LINK

16. Policy Review

This policy will be reviewed every 3 years by the Estates & Infrastructure Committee, or as required to ensure it remains compliant with relevant legislation and best practices.

17. Contact Information

For any questions or concerns regarding this policy or data protection practices, please contact the Data Protection Officer at dataprotection@aaschool.ac.uk

18. Related Policies:

Data Privacy Impact Assessment
Information Security Policy
Membership Fair Processing Policy
Data Retention Policy (GDPR and DPA 2018)
School Fair Processing Notice
Staff Fair Processing Notice
Data Breach Notification