Ambition Institute

Data Protection Policy

Ambition Institute Data Protection Policy

Last reviewed	August 2023
Next review due	August 2024
Responsible division	Compliance
Responsible director	Su Dutta
Applies to	All Employees and external stakeholders
Exceptions	N/A
Audience	All employees and external stakeholders
Applicable laws	UK General Data Protection Regulation (2018) Data Protection Act 2018

Contents

1. Introduction

The purpose of this Policy is to confirm Ambition Institute's ("Ambition", "we") commitment to comply with the UK Data Protection legislation when processing personal data. Data Protection legislation means the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) and any updated legislation.

2. Scope

This policy applies to any processing of Personal Data by Ambition and our partner organisations and to all Personal Data whether stored electronically or in paper copy. The policy applies to all data we hold relating to identified, or identifiable living individuals.

Ambition processes personal information of employees (past and current), contractors, participants in training programmes (applicants, trainees), coaches (including mentors and lead mentors), facilitators, contacts from Lead Partners, HEIs and participating schools and other individuals who come into contact with Ambition Institute.

The Data Protection Policy applies to all Ambition employees, volunteers or contractors that may collect, use, retain, and/or disclose Personal Data. Although third parties are not directly bound by the requirements of this Policy, Ambition is committed to ensuring our suppliers and providers of services embrace the same standards of Data Protection that are consistent with our high standards.

3. Key Definitions

Data Controller means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

Data Processor means a natural or legal person, public authority, agency, or other body, which processes Personal Data on behalf of the Data Controller.

Data Protection Officer is appointed to assist an organisation to monitor internal compliance, inform and advise on Data Protection obligations and act as a contact point for Data Subjects and the Information Commissioner's Office (ICO). Our DPO can be contacted at dataprotection@ambition.org.uk.

Data Subject is an identifiable living natural person who can be identified, directly or indirectly from the Personal Data.

Information Commission Office (ICO) is the UK regulatory supervisory authority for Data Protection legislation in the UK.

Personal Data is defined as information, which relates to a living individual (Data Subject) from which the individual can be identified either directly or indirectly. It includes such information as name, address, email address, date of birth but also can include information such as identification numbers (NI, passport number) or IP addresses.

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.

Processing is any operation or set of operations which is performed on Personal Data, or on sets of Personal Data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Special Category Data includes information about an individual's:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership (or non-membership),
- health data,
- sex life or sexual orientation,
- genetic and biometric information.

For the purposes of this policy, Special Category Data also includes criminal convictions and criminal offences data.

4. Data Protection Principles

The UK GDPR is based on six principles which are to be considered when processing Personal Data. Under the UK GDPR, Article 5 (1) Personal Data should:

- Be processed fairly, lawfully and transparently,
- Be collected and processed only for specified, explicit and legitimate purposes,
- Be adequate, relevant and limited to what is necessary for the purposes for which it is processed,
- Be kept accurate and up to date and any inaccurate data must be deleted or rectified without delay,
- Be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed,
- Be processed in a manner that ensures appropriate security, using appropriate technical and organisational measures.

Ambition is committed to maintaining these principles. This means that we will:

- Identify our lawful basis for collecting and processing data and ensure that we are open with data subjects on how their data will be used.
- Ensure that data processing is in line with the purpose for which it was originally collected.
- Ensure that we only collect data that is relevant and useful.
- Check the quality and accuracy of the information we hold.
- Regularly review the records we hold to ensure that information is not held longer than is necessary and ensure that when information is authorised for disposal it is done appropriately.
- Ensure appropriate security measures to safeguard personal information whether that is held in paper files or on our computer system.
- Document policies, processes and decisions relating to personal data.

Additionally, the UK GDPR Article 5 (2) requires organisations to demonstrate compliance with all the above principles and is sometimes known as the seventh principle.

5. Data Controller Responsibilities

Ambition is classified as a Data Controller and as such we are responsible for ensuring that our data processing activities comply with Data Protection legislation. As a Data Controller, we must:

- Comply and demonstrate compliance with all the GDPR and DPA requirements,
- Ensure our data processors are compliant,
- Co-operate fully with the ICO,
- Implement appropriate organisational and technical measures to ensure data is secure,
- Manage Data Breaches and notify the ICO where appropriate,
- Manage Data Subjects' rights requests efficiently and within specified timeframes; and,
- Pay the Data Protection registration fee and maintain our registration.

The Trustees have overall responsibility for this policy and that any breaches are reported to the Information Commissioner's Office as required.

Ambition senior management, and all those in managerial or supervisory roles, are responsible for developing and encouraging good information handling practice within the company.

Everyone who works for, or with, Ambition has responsibility for ensuring Personal Data is processed in accordance with Data Protection legislation. Non-compliance with this policy may result in disciplinary action.

6. Lawful Bases

When processing any Personal Data, we will establish a lawful basis for processing the information. Employees must ensure that any new processing of Personal Data for which they are responsible, has a written lawful basis approved by senior management and the Data Protection Officer.

When processing Personal Data, one of the following conditions for processing, set out in UK GDPR Article 6, must apply:

- **Consent** Article 6(1)(a))
  We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.
- **Contract** Article 6(1)(b))
  Processing is necessary to fulfil or prepare a contract for the individual.
- **Legal obligation** Article 6(1)(c))
  Processing is necessary to meet a legal obligation.
- **Vital interests** Article 6(1)(d))
  Processing is necessary to protect a person's life or in an urgent medical situation.
- **Public function** Article 6(1)(e))
  Processing is necessary to carry out a public function, a task of public interest, or the function has a clear basis in law assigned to us.
- **Legitimate interest** Article 6(1)(f))
  Processing is necessary for the business/organisation's legitimate interests. This condition does not apply if there is a good reason to protect the individual's Personal Data which overrides the legitimate interest.

The UK GDPR sets a high standard for consent and means giving individuals genuine choice and ongoing control over how we use their Personal Data and ensuring we are transparent. Consent must be:

- informed
- obtained through clear and concise language
- specific
- unambiguous
- freely given
- able to be withdrawn as easily as consent granted
- regularly refreshed

When processing any Special Category Data, we will establish a further condition for processing this data, set out in the UK GDPR Article 9. Employees must ensure that any new processing of Special Category Data for which they are responsible, has a written lawful basis approved by senior management and the Data Protection Officer.

When processing Special Category Data, one of the following conditions must apply:

- **Explicit Consent** Article 9(2)(a))
  We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.
- **Employment Law** Article 9(2)(b))
  Processing is necessary to meet obligations relating to employment, social security, and social protection law.
- **Vital interests** Article 9(2)(c))
  Processing is necessary to protect a person's life or in an urgent medical situation.
- **Not-For-Profit Processing** Article 9(2)(d))
  Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim.
- **Manifestly Public** Article 9(2)(e))
  The Data Subject has already made the Personal Data manifestly public.
- **Legal Claims** Article 9(2)(f))
  Processing is necessary for the organisation to establish, exercise, or defend against legal claims.
- **Substantial Public Interest** Article 9(2)(g))
  Processing is necessary where there is a substantial public interest as specified by domestic/national legislation.
- **Healthcare** Article 9(2)(h))
  Processing is necessary to provide health or social care, or to assess the working capacity of an employee.
- **Public Health** Article 9(2)(i))
  Processing is necessary to protect public health.
- **Research** Article 9(2)(j))
  Processing is necessary for the purposes of archiving, scientific or historical research.

Information about criminal convictions and/or offences

We may only use information relating to criminal convictions or offences where the law allows us to do so. This will usually be where such processing is necessary to carry out our safeguarding obligations and provided we do so in line with Data Protection legislation. We will treat any such data as special category data.

7. Privacy Notices

In order to provide Data Subjects with transparency information as required by UK GDPR Article 5 (1)(a), Article 13 and Article 14, Ambition maintains appropriate privacy notices.

8. Data Subject Rights

Data Subjects have rights in respect of their Personal Data held by Ambition which we must respect and comply with to the best of our ability. Any requests from individual's wanting to exercise their rights should be referred to the DPO as soon as possible.

The following rights can be exercised by Data Subjects:

- **Right to be informed** by the provision of a privacy notice when personal information is processed.
- **Request access** to personal information (commonly known as a "data subject access request"). This enables Data Subjects to receive a copy of the personal information we hold about them and to check that we are lawfully processing it.
- **Request rectification** of the personal information that we hold about Data Subjects. This enables any incomplete or inaccurate information we hold to be corrected.
- **Request erasure** of personal information. This enables Data Subjects to ask us to delete or remove personal information where there is no good reason for us continuing to process it. Data Subjects also have the right to ask us to delete or remove their personal information where they have exercised their right to object to processing.
- **Right to object to processing** of personal information where we are relying on a legitimate interest (or those of a third party) and there is something about the Data Subject's situation which makes them want to object to processing on this ground. Data Subjects also have an absolute right to object where we are processing their personal information for direct marketing purposes.
- **Request the restriction of processing** of personal information. This enables Data Subjects to ask us to suspend the processing of personal information about them.
- **Request the transfer** of personal information to another third party organisation.
- **Automated decision making, including profiling.** The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning or significantly affecting them.

Generally, there is no requirement to pay a fee to exercise any of the legal rights. However, we are entitled to charge a reasonable fee or refuse a request if it is clearly unfounded, repetitive or excessive. We may need to request information to confirm the identity of the requester, in order to make sure that personal data is not disclosed to someone who is not entitled to have it.

A request should be responded to within one month but, if the request is very complex or numerous then we are legally able to extend the request by an additional two months.

Where the processing takes place on the lawful basis of consent, Data Subjects also have the right to withdraw their consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. Ambition are also obliged to inform Data Subjects that they have the right to lodge a complaint with the relevant Supervisory Authority (the ICO in the UK).

9. Data Breaches

Article 4 (12) of the UK GDPR defines a data breach as:

"a breach of security leading to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

A personal data breach can be broadly defined as a security incident which has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

In the event that a personal data breach occurs, it should be reported to the responsible director and Head of Compliance without delay.

Ambition has policies and procedures in place to ensure breaches are escalated to management and the Data Protection Officer as soon as we have become aware of a breach. For externally reportable breaches, Ambition has a legal obligation to report the data breach to the relevant supervisory authority within 72 hours.

Ambition train all our employees in respect of Data Protection legislation and Information Security which are mandatory training sessions for all new staff and annually refreshed for all existing staff. Non-completion of the training may be treated as a disciplinary matter.

10. Security

Ambition will take appropriate steps to ensure that all members of staff and any third-party partners only have access to personal data where it is necessary for them do so. All staff will be made aware of this Policy and their duties under the UK GDPR and DPA. Ambition will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

11. Third Parties

As a Data Controller, Ambition will only transfer Personal Data to third party Data Processors in accordance with UK GDPR Article 28 to ensure we have sufficient guarantees from the provider that the privacy of Data Subjects will be respected and protected. Ambition will ensure that, where Personal Data is transferred to and accessed by third parties, the following actions are completed:

- Ambition will evaluate the third party against a due diligence process, reviewed and approved by Ambition, which assesses privacy risk,
- Ambition will enter into a written contract, reviewed and approved by Ambition with the third party that contains the appropriate data privacy clauses set out in Article 28 and,
- Ambition will maintain detailed records of all third-party contracts

Ambition is also required to share data with the Department for Education and other partners, HEIs Lead Partners. Personal information will only be shared where it is necessary for this purpose.

12. International Transfers

Where Personal Data is transferred outside of the UK to a third party, Ambition will ensure that one of the following measures is in place:

- An adequacy decision between the UK and the third country,
- Standard Contractual Clauses between the data exporter (e.g., Ambition) and the data importer (e.g., third party Data Processor) as well as a Transfer Impact Assessment (TIA) and the UK Addendum,
- UK International Data Transfer Agreement (IDTA) and a Transfer Risk Assessment (TRA),
- Binding Corporate Rules within a multinational organisation transferring data between different national legal entities of the same group,
- Derogations and exceptions for limited, one-time transfers in specific situations.
- Ambition will maintain detailed records of all international transfers within its RoPA, IAR, and Contract Tracker documentation.

13. Data Protection Impact Assessments (DPIAs)

Article 35 of the UK GDPR requires organisations such as Ambition to undertake Data Protection Impact Assessments (DPIAs) in certain circumstances. A DPIA is required to assess privacy risks where there is likely to be a high risk to the rights and freedoms of the Data Subjects involved. In practice, this means that any time Ambition processes Personal Data for a new purpose or using a new system, we will consider whether a DPIA is required. If a DPIA is not required, Ambition will document this decision through the completion of a DPIA screening tool document. If a DPIA is required, we will conduct the assessment before any data processing activities commence.

14. Data retention

Ambition will only retain personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of personal data information will be documented.

15. Marketing

Ambition will abide by the UK GDPR and PECR rules in respect of our marketing communications. All new marketing communications which are construed as 'direct marketing' (directly contacting specific individuals to offer goods and services, or to promote the goals of Ambition) will be reviewed and approved by the Marketing Lead and the DPO before communication to the Data Subject.

16. Training

Employees will receive adequate training on the provisions of Data Protection law relevant to their role. Our employees will complete all training as requested and if they move role or have additional responsibilities, they will receive additional appropriate Data Protection training as required.

17. Audits

Regular data audits to manage and mitigate risks will be carried out as required. This includes information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. The DPO will conduct regular data audits as required by applicable Data Protection legislation or where there is an identified business need.

18. Data Protection and Filming

Ambition will supply appropriate guidance regarding data protection to anyone involved in filming, particularly in school settings.

Photographs with names identifying participants, coaches or pupils will not be published on our website or in other marketing material without the explicit consent of the individuals concerned.

19. Monitoring Compliance

All staff must observe this Data Protection Policy. The DPO has overall responsibility for the policy and will keep it under regular review and will amend or change it as required. Any breaches of the policy must be notified to the DPO. Adherence to this policy is mandatory and must be followed at all times. Non-compliance with this policy by our employees or contractors will be treated seriously by Ambition and may amount to gross misconduct ultimately resulting in dismissal.

20. Disclosing Data for Other Reasons

In certain circumstances, Data Protection legislation allows personal data to be disclosed to third parties, such as the Courts, Government agencies or Law Enforcement agencies without the consent of the Data Subject. Under these circumstances, Ambition will disclose the data as required by the law. However, the DPO will review all such requests to ensure compliance with the relevant legislation.

21. Contact and Complaints

Please contact the DPO if you have any queries regarding this policy at dataprotection@ambition.org.uk

If you still have concerns about how we are handling your personal data, then you can contact the Information Commissioner's Office by visiting ico.org.uk or by telephoning 03039 1231113 or by writing to the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.