THE AI BOARD

POLICY · POL / DATAPRO

Data Protection *Policy.*

The AI Board's commitment to protecting the rights and freedoms of individuals with respect to the processing of their personal information — in compliance with the Data Protection Act 2018 and the UK's implementation of the GDPR.

VERSION	ISSUE DATE	REVIEW DATE	AUTHOR
v0.2	October 2024	March 2026	J Jones / R Palmer

SECTION 01

Introduction

The AI Board is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal information.

The organisation needs to collect and use certain types of information about job applicants, learners, employees and other individuals (data subjects) who work with The AI Board or come into contact with it.

This information will be obtained for a relevant purpose and will be collected and retained to meet that purpose. It will be dealt with appropriately however it is collected, recorded and used; whether on paper, electronic or recorded on other material and it will be safeguarded to ensure we comply with relevant legislation.

The information will not be held longer than is necessary. The AI Board regards the lawful and correct treatment of personal information as a priority and therefore it will ensure that this information is treated correctly. The AI Board will process and control such information primarily for recruitment, registration, assessment, certification, analysis, personnel, marketing, administrative, regulatory and payroll purposes.

> This policy is intended to comply with the **Data Protection Act of 2018** and the UK's implementation of the **General Data Protection Regulation (GDPR)**.

Under the Act, there is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

SECTION 02

Scope

This policy applies to all stakeholders of The AI Board.

This policy does not form part of the formal employee contract nor of the centre contract with The AI Board, but it is a condition of both that the rules and policies made by The AI Board will be complied with. Any failure to comply with this policy will be dealt with in a formal manner.

All employees, centres and other data subjects are entitled to:

- Know what information the centre holds and processes about them and why
- Know how to gain access to it
- Know how to keep it up to date
- Know what the centre is doing to comply with its legal obligations
- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

SECTION 03

Implementation of the Policy

Data Security

All employees and associates are responsible for ensuring that:

- Any personal data which they hold is kept and disposed of securely
- Personal information is not disclosed either orally, in writing accidentally or otherwise to any unauthorised third party
- Employees and associates should note that unauthorised disclosure will usually be dealt with formally.

Personal information must be:

- Kept in a locked office, filing cabinet or drawer

Password protected when stored on a computer

Secure if it is held on a portable device

Unauthorised Access

Any employee, associate, learner or other stakeholder who deliberately gains or attempts to gain unauthorised access to personal data on any data subject or discloses such data to any third party will be dealt with formally in accordance with The AI Board procedures.

Centre Obligations

Centres must ensure that all data provided to The AI Board is accurate and up to date. This includes data relating to the organisation, its staff and any learners registered.

Rights of Access to Information

Employees, learners and other data subjects have the right of access to any personal data that is being kept about them either electronically or in other files.

Certain disclosures may be made without consent so long as the information is requested by an appropriate Government or regulatory authority for one or more of the following purposes (requests must be supported by appropriate paperwork):

- to safeguard national security
- prevention or detection of crime including the apprehension or prosecution of offenders
- assessment or collection of tax duty
- discharge of regulatory functions (includes health, safety and welfare of persons at work)
- to prevent serious harm to a third party
- to protect the vital interests of the individual, this refers to life and death situations

Retention of Data

The AI Board will only hold data on individuals as long as we deem it necessary to carry out a particular activity. Information about staff will be retained for at least six years after they leave The AI Board. However, some information will be held for a longer period, for example data which relates to tax or pensions and any references provided. The AI Board will maintain a Data Processing Log, in line with Article 30 of the GDPR to manage all data retained by the company.

Data Protection Impact Assessments (DPIAs)

The AI Board has a process for conducting DPIAs when initiating new projects or processing activities which could pose potential risk to individuals' rights and freedoms. DPIAs will be undertaken on all relevant policies and procedures and a DPIA report logged in a central record.

Data Protection Officer (DPO)

In line with guidance under the GDPR, The AI Board will appoint a Data Protection Officer.

Responsibilities of the DPO will include:

- Monitoring compliance with GDPR and data protection policies.
- Advising on data protection impact assessments (DPIAs).
- Training staff and raising awareness about data protection.

Acting as a contact point for data subjects and regulatory authorities like the Information Commissioner's Office (ICO).

Ensuring lawful processing of personal data.

Training and Awareness

The AI Board will establish regular training programs to ensure all staff and stakeholders understand their responsibilities under data protection laws. This fosters a culture of compliance and vigilance.

SECTION 04

Conclusion

Any stakeholders who wish to clarify the contents of this policy should speak to the Chief Executive of The AI Board. Anyone who considers that this policy has not been followed in respect of personal data about themselves or about other data subjects can raise the matter, using The AI Board's formal complaints procedure.

> All stakeholders involved in working with The AI Board in any way will uphold both the policy and the practice outlined in this policy and remain, at all times, within the guidance given in the 2018 Act and the General Data Protection Regulation (GDPR).

SECTION 05

Review

DOC ID	TITLE	WORK AREA	VERSION	ISSUE DATE	REVIEW DATE	AUTHOR	OFQUAL RELATED
POL	DATAPRO	ADM	v0.2	October 2024	March 2026	J Jones / R Palmer	Y

Version Control

VERSION NUMBER	SUMMARY OF CHANGE	DATE CHANGED	NEW REVIEW DATE