Appendix 9 - Appropriate Policy Document

- **About this policy**

This is the "appropriate policy document" for Initio Learning Trust setting out how we will protect Special Categories of Personal Data and Criminal Convictions Data.

Where we process other Special Categories of Personal Data and Criminal Convictions Data in instances where there is no requirement to keep an appropriate policy document, we will process it on a basis that respects the rights and interests of Data Subjects. Further information in respect of this processing can be found within our privacy notices [include links].

This policy supports Initio Learning Trust's Data Protection Policy and adopts its definitions and should be read in conjunction with that policy.

- **Definitions**

Controller: is the person who or organisations which determine the purposes for which, and the means by which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own purposes

Criminal Convictions Data: personal data relating to criminal convictions and offences, including Personal Data relating to criminal allegations and proceedings and sentencing.

Data Retention Policy: explains how the organisation classifies and manages the retention and disposal of its information. Time periods for retention are set out in the retention schedule.

Data Subject: for the purpose of this policy include all the identified or identifiable living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.

DPA 2018: the Data Protection Act 2018.

Data Protection Officer (DPO): as set out in our Data Protection Policy, as a Trust the person we have appointed to be responsible for ensuring compliance with the DPA 2018 and the UK GDPR, as our DPO is Tracy Broadbent, and they can be contacted at privacy@initiolearning.org.

UK GDPR: the retained EU law version of the General Data Protection Regulation (*(EU) 2016/679*).

Personal Data: any information relating to an identified or identifiable living individual (a data subject); an identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or

to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual. Personal Data includes Special Categories of Personal Data.

Privacy Notice: a separate notice required to be provided to Data Subjects which is usually given at the point the organisation collects information about them. For Initio Learning Trust this includes privacy notices for Staff, Students and Parents, Job Applicants, Visitors and Contractors and for Volunteers including those in Governance.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transmitting or transferring Personal Data to third parties.

Special Categories of Personal Data: includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.

- **Why we process Special Categories of Personal Data and Criminal Convictions Data**

We process Special Categories of Personal Data and Criminal Convictions Data for the following purposes where this is in accordance with our Data Protection Policy:

(a) to carry out our legal obligations in relation to employment law;

(b) for the purposes of preventative or occupational medicine in order to assess an employee's working capacity and/or the need for reasonable adjustments;

(c) complying with health and safety obligations;

(d) complying with the Equality Act 2010 and in the interests of ensuring equal opportunities and treatment;

(e) checking applicants' and employees' right to work in the UK;

(f) verifying that candidates are suitable for employment or continued employment;

(g) to administer and pay trade union premiums and register the status of a protected employee;

(h) to safeguard our pupils and other individuals;

(i) to support individuals with a particular disability or medical condition;

(j) in relation to legal claims;

(k) to protect the data subject’s vital interests where they are not able to provide their consent;

(l) to prevent or detect crime without the consent of the data subject so as not to prejudice those purposes where it is necessary for reasons of substantial public interest.

- **Personal data protection principles**

The UK GDPR requires personal data to be processed in accordance with the six principles set out in Article 5(1). Article 5(2) requires controllers to be able to demonstrate compliance with Article 5(1).

We comply with the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

(a) processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);

(b) collected only for specified, explicit and legitimate purposes (Purpose Limitation);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);

(d) accurate and where necessary kept up to date (Accuracy);

(e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation); and

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

- **Compliance with data protection principles**

1. Lawfulness, fairness and transparency

Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

We will only Process Personal Data fairly and lawfully and for specified purposes. We will only Process Special Categories of Personal Data and Criminal Convictions Data where we have a lawful basis for Processing and one of the specific conditions relating to Special Categories of Personal Data or Criminal Convictions Data applies. We will identify and document the legal basis and specific Processing condition relied on for each Processing activity below.

When collecting Special Categories of Personal Data and Criminal Convictions Data from Data Subjects, either directly from Data Subjects or indirectly (for example from a third party or publicly available source), we will provide Data Subjects with a Privacy Notice setting out all the information required by

the UK GDPR in a concise, transparent, intelligible, easily accessible manner and in clear plain language which can be easily understood.

Type of Special Categories of Personal Data/Criminal Convictions Data Processed	**Lawful basis for Processing**	**Condition for processing Special Categories of Personal Data/Criminal Convictions Data**
Data concerning health	Compliance with a legal obligation (*Article 6 (1)(c)*) or necessary for the performance of a contract with the Data Subject (*Article 6(1)(b)*) or processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6(1)(e)).	Necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the Data Subject in connection with employment, social security or social protection. (*Paragraph 1(1)(a), Schedule 1, DPA 2018*.) Necessary for health and social care purposes. (*Paragraph 2(1), Schedule 1, DPA 2018*.) To provide support for individuals with a particular disability or medical condition. (*Paragraph 16(1), Schedule 1, DPA 2018*.) Necessary for the provision of confidential counselling, advice or support or of another similar service provided confidentially. (*Paragraph 17(1), Schedule 1, DPA 2018*.)
Racial or ethnic origin data	Compliance with a legal obligation (*Article 6(1)(c)*).	Necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the Data Subject in connection with employment, social security or social protection. (*Paragraph 1(1)(a), Schedule 1, DPA 2018*.)

Criminal Convictions Data	Compliance with a legal obligation (*Article 6(1)(c)*). **OR** In the organisation's legitimate interests (*Article 6(1)(f)*) which are not outweighed by the fundamental rights and freedoms of the Data Subject.	Necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the Controller or the Data Subject in connection with employment, social security or social protection. (*Paragraph 1(1)(a), Schedule 1, DPA 2018*.) Meets one of the substantial public interest conditions set out in Part 2 of Schedule 1 to the DPA 2018 (such as: ● preventing or detecting unlawful acts (*Paragraph 10(1), Schedule 1, DPA 2018*.) ● protecting the public against dishonesty etc. (*Paragraph 11(1), Schedule 1, DPA 2018*.) ● complying with, or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another persona has committed an unlawful act; or been involved in dishonesty, malpractice or other seriously improper conduct (*Paragraph 12(1), Schedule 1, DPA 2018*.) ● preventing fraud or a particular kind of fraud .(*Paragraph 14(1), Schedule 1, DPA 2018*.) Necessary for the purposes of: ● protecting an individual from neglect or physical, mental or emotional harm, or

		• protecting the physical, mental or emotional well-being of an individual where the individual is under the age of 18, or is 18 or over and at risk. .(*Paragraph 18(1), Schedule 1, DPA 2018*.)
Equal opportunity data	In the organisation's legitimate interests (*Article 6(1)(f)*) which are not outweighed by the fundamental rights and freedoms of the Data Subject.	Necessary for the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained. (*Paragraph 8(1)(b), Schedule 1, DPA 2018*.)
Biometric data	Compliance with consent (*Article 6 (1)(a)* Consent is to be freely given, informed, unambiguous, specific (granular) and a clear affirmative action.	Explicit Consent

2. Purpose limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

We will only collect Personal Data for specified purposes and will inform Data Subjects what those purposes are in a published Privacy Notice. If we plan to use personal data for a new purpose (other than a legal obligation or function set out in law) we will check that this is compatible with our original purpose. We will not use Personal Data for new, different or incompatible purposes from those disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have consented where necessary.

3. Data minimisation

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

We will only collect or disclose the minimum Personal Data required for the purpose for which the data is collected or disclosed. We will ensure that we do not collect excessive data and that the Personal Data collected is adequate and relevant for the intended purposes. We will periodically review the Personal Data and delete anything we don't need.

4. Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

We will ensure that the Personal Data we hold and use is accurate, complete, kept up to date and relevant to the purpose for which it is collected by us. We check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data. These include annual data checks for staff and students

As set out in our Data Protection Policy, Data Subjects have the right to rectification. Our Data Protection Policy which can be found at https://www.initiolearning.org/about-initio/policies-and-documents confirms how the Trust considers and complies with any request to the right to rectification.

5. Storage limitation

We only keep Personal Data in an identifiable form for as long as is necessary for the purposes for which it was collected, or where we have a legal obligation to do so. Once we no longer need Personal Data it shall be deleted or rendered permanently anonymous.

We maintain a Data Retention Policy and related procedures to ensure Personal Data is deleted after it is no longer needed for the purposes for which it was being held, unless we are legally required to retain that data for longer.

We will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

6. Security, integrity, confidentiality

Personal Data shall be Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. We will analyse any risks presented by our Processing to assess the level of security required.

- **Entry controls**. Any stranger seen in entry-controlled areas should be reported to the head teacher.

- **Secure lockable desks and cupboards**. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

- **Methods of disposal**. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the Information Commissioner's Office guidance on the disposal of IT assets.

■ **Equipment**. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

■ **Working away from the school premises – paper documents must not be removed from school unless required for an educational visit.**

■ **Working away from the school premises – electronic working**. staff must only use secure devices provided by the Trust.

■ **Document printing** - Documents containing Special Categories of **Personal Data** must be collected immediately from printers and not left on photocopiers.

■ **Multifactor authentication** is used for all systems where Special Categories of Personal Data/Criminal Convictions Data is processed.

■ **Biometric data** is stored as a mathematical algorithm that cannot be recreated into a fingerprint image.

■ **Medical information** can only be processed by staff assigned the appropriate business role. Business roles are reviewed monthly by the Trust Data Manager and DPO.

7. Accountability principle

We are responsible for, and able to demonstrate compliance with these principles. Our DPO is responsible for ensuring that we are compliant with these principles. Any questions about this policy should be submitted to the DPO. We also have appropriate data protection policies in place, such as a Retention Policy, Data Breach Policy, Biometrics Policy, CCTV Policy, Subject Access Request Policy and Record of Processing Activities.

We will:

(a) Ensure that records are kept of all Personal Data Processing activities, and that these are provided to the Information Commissioner on request.

(b) Carry out a DPIA for any Personal Data Processing that is likely to result in a high risk to Data Subjects' interests to understand how Processing may affect Data Subjects and consult the Information Commissioner if appropriate.

(c) Ensure that a DPO is appointed to provide independent advice and monitoring of Personal Data handling, and that the DPO has access to report to the highest management level.

(d) Have internal processes to ensure that Personal Data is only collected, used or handled in a way that is compliant with these principles.

- **Controller's policies on retention and erasure of personal data**

We will ensure, where Special Categories of Personal Data or Criminal Convictions Data are Processed so that:

(a) Where we no longer require Special Categories of Personal Data or Criminal Convictions Data for the purpose for which it was collected, we will delete it or render it permanently anonymous as soon as possible.

(b) Where records are destroyed we will ensure that they are safely and permanently disposed of.

Data Subjects receive a Privacy Notice setting out how their Personal Data will be handled when we first obtain their Personal Data, and this will include the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period. The Privacy Notice is also available on our website.

- **Review**

This policy on Processing Special Categories of Personal Data and Criminal Convictions Data is reviewed annually. No condition for processing and associated information will be removed from this policy until the expiry of 6 months following the end of the period during which the Trust undertakes that processing activity.

The policy will be retained where we process Special Categories of Personal Data and Criminal Convictions Data and any earlier versions will be retained for a period of at least six months after we stop carrying out such processing.

A copy of this policy will be provided to the Information Commissioner on request and free of charge.