



## DATA PROTECTION POLICY

### **Fresh Start in Education Limited**

Castle House | Castle Hill Avenue | Ground Floor | Folkestone | Kent | CT20 2TQ



## CONTENTS

1. Introduction	3
2. The Data Protection Principles	4
3. Lawful, Fair and Transparent Data Processing	4
4. Processed for Specified, Explicit and Legitimate Purposes	5
5. Adequate, Relevant and Limited Data Processing	5
6. Accuracy of Keeping Data Up to Date	5
7. Timely Processing	5
8. Secure Processing	5
9. Accountability	5
10. Privacy Impact Assessments	6
11. The Rights of Data Subjects	6
12. Keeping Data Subjects Informed	6
13. Data Subject Access	7
14. Rectification of Personal Data	7
15. Erasure of Personal Data	8
16. Restriction of Personal Data Processing	8
17. Objections to Personal Processing	8
18. Automated Decision Making	9
19. Profiling	9
20. Personal and Special Category Data	9
21. Data Protection Measures	14
22. Organisational Measures	16
23. Transferring Personal Data to a Country Outside the EEA	16
24. Data Breach Notification	16
Implementation of Policy	17

## DEFINITIONS

- Fresh Start in Education Ltd will be referred to as ‘the Company’ throughout the policy
- The term ‘staff’ is used to cover all Company employees, contractors and workers, past and present
- The term ‘student’ is used to cover any learner placed with the Company, at anytime
- The term ‘Client’ refers to any local authority, school, parent or body that commissions the services of the Company to work with a student or students
- An ‘Identifiable Natural Person’ 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 natural person
- A ‘Data Subject’ is the identified or Identifiable Natural Person to which the data refers
- ‘Data Controller’ is a natural or legal person, Public Authority, Agency or other body which, alone or jointly with others, determines the purpose and means of the Processing of Personal Data
- A ‘Data Processor’ is a natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller
- ‘Personal Data’ is any information that relates to a living individual who can be identified from that information
- The ‘Data Protection Officer’ (DPO), is Dan Parrett and the ‘Deputy Data Protection Officer’ (DDPO) is Emily Wolstenholme - they may be contacted in writing;  
The Data Protection Officer  
Fresh Start in Education Ltd  
Castle House  
Castle Hill Avenue  
Folkestone  
Kent. CT20 2TQ  
or by email: [dataprotectionofficer@freshstartedu.co.uk](mailto:dataprotectionofficer@freshstartedu.co.uk)
- The terms ‘processing’, ‘process’ or ‘processed’ are used to cover any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include 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.

## 1. INTRODUCTION

The Company is a specialist Interim Engagement and Education Service. We work with some of the most vulnerable children and young people and work to a high standard of Safeguarding and Data Protection. The services of the Company are commissioned by Local Authority Departments, Schools and Colleges and occasionally parents or carers themselves. All data processed by the Company is for the purpose of fulfilling our Contract with the body that commissions our services.

We hold data for up to 85 years for a variety of reasons, but this is not for marketing purposes with the exception of those who have or may commission our services. Data is processed as necessary by the Company’s staff members to ensure that the students placed with us get the maximum benefit from their time with us and are safe guarded effectively. We use historic data to review and assess our effectiveness with different groups of students and their progress and the outcomes that they have achieved. We also keep all data to ensure that we can respond effectively to any Safeguarding matter or questions concerning behaviour, or effectiveness of staff or service.

This policy sets out the obligations of the Company regarding Data Protection and the rights of Clients, staff, and students, in respect of their Personal Data under the General Data Protection Regulation

("the Regulation").

This policy sets out the procedures that are to be followed when dealing with Personal Data. The procedures and principles set out herein must be followed at all times by staff.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all Personal Data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

## **2. THE DATA PROTECTION PRINCIPLES**

This policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling Personal Data must comply. All Personal Data must be:

- Processed lawfully, fairly, and in a transparent manner in relation to the Data Subject
- Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay
- Kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the Data Subject
- Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

## **3. LAWFUL, FAIR AND TRANSPARENT DATA PROCESSING**

The Regulation seeks to ensure that Personal Data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the Data Subject. The Regulation states that processing of Personal Data shall be lawful if at least one of the following applies:

- The Data Subject has given consent to the processing of his or her Personal Data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject
- Processing is necessary to protect the vital interests of the Data Subject or of another Identifiable Natural Person
- 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 Data Controller
- Processing is necessary for the purposes of the Legitimate Interests pursued by the Data Controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the Data Subject, which require protection of Personal Data, in particular where the Data Subject is a child.

#### **4. PROCESSED FOR SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES**

The Company collects and processes the Personal Data set out in Point 20 of this policy. This may include Personal Data received directly from Data Subjects, for example, contact details used when a Data Subject communicates with us and data received from third parties, for example, Local Authority departments, Police, the Courts, schools, teaching and support staff and parents, carers, family members and those connected with a student or their family who are providing information about students with whom the Company is working, has worked, or may be required to work. It may also include information from social media or other sources and where there may be Safeguarding or Behaviour concerns.

The Company only processes Personal Data for the specific purposes set out in Point 20 of this policy or for other purposes expressly permitted by the Regulation. The purposes for which we process Personal Data will be informed to Data Subjects at the time that their Personal Data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

#### **5. ADEQUATE, RELEVANT AND LIMITED DATA PROCESSING**

The Company will only collect and process Personal Data for and to the extent necessary for the specific purpose(s) informed to Data Subjects as under Point 4, above.

#### **6. ACCURACY OF KEEPING DATA UP TO DATE**

The Company shall ensure that all Personal Data collected and processed is kept accurate and up-to-date. The accuracy of Personal Data shall be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend, erase or anonymise that data, as appropriate.

#### **7. TIMELY PROCESSING**

The Company shall not keep Personal Data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to anonymise or erase it without delay.

#### **8. SECURE PROCESSING**

The Company shall ensure that all Personal Data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Points 21 and 22 of this policy.

#### **9. ACCOUNTABILITY**

The Company shall keep written internal records of all Personal Data collection, holding, and processing, which shall incorporate the following information:

- The name and details of the Company, its DPO, and any applicable third-party Data Controllers
- The purposes for which the Company processes Personal Data
- Details of the categories of Personal Data collected, held, and processed by the Company; and the categories of Data Subject to which that Personal Data relates
- Details and categories of any third parties that will receive Personal Data from the Company
- Details of any transfers of Personal Data to non-European Economic Area countries, including all mechanisms and security safeguards
- Details of how long Personal Data will be retained by the Company
- Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of Personal Data.

## **10. PRIVACY IMPACT ASSESSMENTS**

The Company shall carry out Privacy Impact Assessments when and as required under the Regulation, and as part of the annual review of this policy. Privacy Impact Assessments shall be overseen by the Company's DPO and shall address the following areas of importance:

- The purpose(s) for which Personal Data is being processed and the processing operations to be carried out on that data
- Details of the Legitimate Interests being pursued by the Company
- An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed
- An assessment of the risks posed to individual Data Subjects
- Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of Personal Data, sufficient to demonstrate compliance with the Regulation.

## **11. THE RIGHTS OF DATA SUBJECTS**

The Regulation sets out the following rights applicable to Data Subjects:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (also known as the 'right to be forgotten')
- The right to restrict processing
- The right to data portability
- The right to object
- Rights with respect to automated decision-making and profiling.

## **12. KEEPING DATA SUBJECTS INFORMED**

The Company shall ensure that the following information is provided to every Data Subject when Personal Data is collected:

- Details of the Company including, but not limited to, the identity of the DPO
- The purpose(s) for which the Personal Data is being collected and will be processed (as detailed in Point 20 of this policy) and the legal basis justifying that collection and processing
- Where applicable, the Legitimate Interests upon which the Company is justifying its collection and processing of the Personal Data
- Where the Personal Data is not obtained directly from the Data Subject, the categories of Personal Data collected and processed
- Where the Personal Data is to be transferred to one or more third parties, details of those parties
- Where the Personal Data is to be transferred to a third party that is located outside of the European Economic Area (EEA), details of that transfer, including but not limited to the safeguards in place. See Point 23 of this policy for further details concerning such third country data transfers
- Details of the length of time the Personal Data will be held by the Company or, where there is no predetermined period, details of how that length of time will be determined
- Details of the Data Subject's rights under the Regulation
- Details of the Data Subject's right to withdraw their consent to the Company's processing of their Personal Data at any time

- Details of the Data Subject's right to complain to the Information Client's Office (the 'supervisory authority' under the Regulation)
- Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the Personal Data and details of any consequences of failing to provide it
- Details of any automated decision-making that will take place using the Personal Data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

The information set out above shall be provided to the Data Subject at the following applicable time:

- Where the Personal Data is obtained from the Data Subject directly, at the time of collection
- Where the Personal Data is not obtained from the Data Subject directly, for example, from another party:
  - If the Personal Data is used to communicate with the Data Subject, at the time of the first communication, or
  - If the Personal Data is to be disclosed to another party, before the Personal Data is disclosed, or
  - In any event, not more than one month after the time at which the Company obtains the Personal Data.

### **13. DATA SUBJECT ACCESS**

A Data Subject may make a Subject Access Request (SAR) at any time to find out more about the Personal Data which the Company holds about them. The Company is normally required to respond to SARs within one month of receipt. This can be extended by up to two months in the case of complex and or numerous requests, and in such cases the Data Subject shall be informed of the need for the extension.

All SAR's received must be made in writing to the DPO. A SAR must describe the information required and be accompanied by proof of identity to ensure that information is only shared with the Data Subject themselves.

The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a Data Subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

### **14. RECTIFICATION OF PERSONAL DATA**

If a Data Subject informs the Company that Personal Data held by the Company is inaccurate or incomplete, requesting that it be rectified, the Personal Data in question shall be rectified, and the Data Subject informed of that rectification, within one month of receipt the Data Subject's notice. This can be extended by up to two months in the case of complex requests, and in such cases the Data Subject shall be informed of the need for the extension.

In the event that any affected Personal Data has been disclosed to third parties, those parties shall be informed of any rectification of that Personal Data.

## **15. ERASURE OF PERSONAL DATA**

Data Subjects may request that the Company erases the Personal Data it holds about them in the following circumstances:

- It is no longer necessary for the Company to hold that Personal Data with respect to the purpose for which it was originally collected or processed
- The Data Subject wishes to withdraw their consent to the Company holding and processing their Personal Data
- The Data Subject objects to the Company holding and processing their Personal Data, and there is no overriding legitimate interest to allow the Company to continue doing so. See Point 17 of this policy for further details concerning Data Subjects' rights to object
- The Personal Data has been processed unlawfully
- The Personal Data needs to be erased in order for the Company to comply with a particular legal obligation.

Unless the Company has reasonable grounds to refuse to erase Personal Data, all requests for erasure shall be complied with, and the Data Subject informed of the erasure, within one month of receipt of the Data Subject's request. This can be extended by up to two months in the case of complex requests, and in such cases the Data Subject shall be informed of the need for the extension.

In the event that any Personal Data which is to be erased in response to a SAR, has been disclosed to third parties, those parties shall be informed of the erasure, unless it is impossible or would require disproportionate effort to do so.

## **16. RESTRICTION OF PERSONAL DATA PROCESSING**

Data Subjects may request that the Company ceases processing the Personal Data it holds about them. If a Data Subject makes such a request, and unless the Company has reasonable grounds to refuse the restriction of Personal Data, all requests for restriction shall be complied with, and the Data Subject informed of the restriction, within one month of receipt of the Data Subject's request. This can be extended by up to two months in the case of complex requests, and in such cases the Data Subject shall be informed of the need for the extension. The Company shall retain only the amount of Personal Data pertaining to that Data Subject that is necessary to ensure that no further processing of their Personal Data takes place.

In the event that any affected Personal Data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it, unless it is impossible or would require disproportionate effort to do so.

## **17. OBJECTIONS TO PERSONAL DATA PROCESSING**

Data Subjects have the right to object to the Company processing their Personal Data based on Legitimate Interests, including profiling, direct marketing, including profiling, and processing for scientific and or historical research and statistical purposes.

Where a Data Subject objects to the Company processing their Personal Data based on its Legitimate Interests, the Company shall cease such processing forthwith, unless it can be demonstrated that the Company's legitimate grounds for such processing override the Data Subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

Where a Data Subject objects to the Company processing their Personal Data for direct marketing



purposes, the Company shall cease such processing forthwith.

Where a Data Subject objects to the Company processing their Personal Data for scientific and or historical research and statistical purposes, the Data Subject must, under the Regulation, 'demonstrate grounds relating to their particular situation'. The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

## **18. AUTOMATED DECISION MAKING**

In the event that the Company uses Personal Data for the purposes of automated decision-making and those decisions have a legal, or similarly significant effect on Data Subjects, Data Subjects have the right to challenge to such decisions under the Regulation, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Company.

This does not apply in the following circumstances:

- The decision is necessary for the entry into, or performance of, a contract between the Company and the Data Subject
- The decision is authorised by law
- The Data Subject has given their explicit consent.

## **19. PROFILING**

Where the Company uses Personal Data for profiling purposes, the following shall apply:

- Clear information explaining the profiling will be provided, including its significance and the likely consequences
- Appropriate mathematical or statistical procedures will be used
- Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented
- All Personal Data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling. See Points 21 and 22 of this policy for more details on data security.

## **20. PERSONAL AND SPECIAL CATEGORY DATA**

For the purpose of Safeguarding and Child Protection all data relating to students and Parent/Carers listed in this section will be held for up to 85 years.

The following Personal Data may be collected, held, and processed by the Company.

### **20.1. Students and their Parents/Carers**

We keep Personal Data relating to the referral or placement of a student in order to:

- Perform the Contract that we have with the Client and in order to pursue the legitimate business interests of the Company
- Review and assess the effectiveness of the service
- Ensure that we can respond effectively to any questions about the behaviour or progress of students, and the effectiveness of staff or the Company's service
- Ensure that we can properly respond to any safeguarding or legal concerns or enquiries at any time.

Students and their parents/carers Personal Data is never used for direct marketing purposes. Apart from day to day contact with students and their parents/carers during the course of a provision, the only other contact we may have will be to obtain feedback in connection with a provision.

#### **20.2. Clients**

Personal Data, that we hold on those who commission our services, is collected and held to ensure that we can fulfil any Contract, and for the legitimate business interests of the Company. Contact details may be used for direct marketing from time to time to keep Clients and potential Clients up to date with any changes to our services. Clients can choose to opt out from these communications if they wish.

#### **20.3. Applicants**

We keep Personal Data of people who apply to work for us to process their application. Unsuccessful applicant's data is stored for no more than 24 months after they are informed of our decision regarding employment unless it is necessary to keep Personal Data for Public Interest or legal reasons. After 24 months Personal Data is deleted or anonymised, unless retained for reasons given.

#### **20.4. Staff**

Staff Personal Data is kept for up to 85 years.

## 20.5 PERSONAL DATA – Parents/Carers, Clients and students

	<b>Category of Personal Data</b>	<b>Purpose of Processing</b>	<b>Legal Basis for Processing</b>
<b>Parents/Carers</b>	Names, telephone numbers, email addresses and email letter and telephone correspondence, audio recordings of telephone conversations, and any information provided by the Client.	<p>Fulfilment of the Contract with the Client.</p> <p>Safeguarding and Child Protection.</p> <p>Parents/Carers may be contacted from time to time to provide on the effectiveness of the Company's service and as part of the Company's continual improvement, and Quality Assurance.</p>	Legitimate Interest, Legal Obligation, Public Interest and Vital Interest.
<b>Students</b>	Names, addresses, date of birth, telephone numbers, email addresses, next of kin, emergency contact details, education history and plans, religion, disabilities, physical and mental health, medication, gender, sexual orientation, marital status, ethnicity, nationality, relatives' and or carers' contact details, social services contact details and role, Police and other official involvement, general educational and social history, court history and orders, financial information, social media history and interactions, audio recordings of telephone conversations.	<p>Future and current students: Fulfilment of our contract with the referring Client.</p> <p>Past students: Safeguarding and Child Protection, educational, behavioural and engagement history and attainment.</p> <p>Students may be contacted from time to time to provide feedback or to enter competitions to assess the effectiveness of the Company's methods and as part of the Company's continual improvement and Quality Assurance.</p>	Legitimate Interest, Legal Obligation, Public Interest, Vital Interest and Statistical Research and Processing.
<b>Clients</b>	Names, telephone number, email addresses, office address, job title, employer, email, letter and telephone correspondence, audio recordings of telephone conversations, contract(s), tenders, tender submissions, preferences and interests, general financial information relating to the Client body, payment terms and efficiency, usage of the Company's website.	<p>Fulfilment of contract with the Client.</p> <p>Safeguarding, Child Protection and Behaviour Management and Reporting.</p> <p>Statistical Analysis and Review and Quality Assurance.</p>	Legitimate Interest, Legal Obligation, Public Interest, Vital Interest and Research and Statistical Purposes.

## 20.6 PERSONAL DATA – Staff and Applicants

Category of Personal Data (Staff and Applicants)	Purpose of Processing	Legal Basis for Processing	Recipients to whom disclosed
<p>Personal information and contact details, including: name, address, date of birth, gender, marital status, ethnicity, nationality, telephone number, email address and next of kin, emergency contact details, job title, photo, signature, teacher number (where applicable), job title, photo, signature, primary and secondary languages, religion, sexual orientation, email, letter and telephone correspondence, audio recordings of telephone conversations.</p>	<p>To allow the organisation to maintain accurate records and contact details.</p> <p>For HR and business administration purposes.</p> <p>For defence against potential legal claims or safeguarding investigations.</p>	<p>Performance of a contract or to enter into a contract.</p> <p>Legal obligation.</p> <p>Legitimate Interests.</p>	<p>Clients, HR Consultants, Lawyers, and Government organisations as and when required, by law (LADO, Police, etc.,)</p>
<p>Recruitment records, including: CVs, application forms, interview notes, test results, proof of right to work in UK (such as passports and visas), driving licence, evidence of skills and qualifications, references, car MOT, car insurance documents, prohibition of teachers checks, any other relevant checks and audio recordings of telephone conversations.</p>	<p>To assess an individual's suitability for work and to determine to whom to offer employment.</p> <p>To comply with legislative and regulatory requirements.</p> <p>For HR and business administration purposes.</p> <p>For defence against potential legal claims or safeguarding investigations.</p>	<p>Performance of a contract or to enter into a contract.</p> <p>Legal Obligation.</p> <p>Legitimate Interests.</p>	<p>External organisations conducting reference and background checks, HR Consultants and Lawyers.</p>
<p>Recruitment records containing special categories of Personal Data (including details of any disabilities disclosed and reasonable adjustments) and criminal records data (including results of criminal record checks).</p>	<p>To assess an individual's suitability for work and to determine to whom to offer employment.</p> <p>To comply with the requirement to make reasonable adjustments.</p> <p>For HR and business administration purposes.</p> <p>For defence against potential legal claims or safeguarding investigations.</p>	<p>Necessary to carry out obligations or exercise rights under employment law.</p> <p>Legitimate Interests.</p>	<p>External organisations conducting reference and background checks, HR Consultants and Lawyers.</p>

<p>Offer letters, contracts of employment, written statements of terms and related correspondence.</p>	<p>To maintain a record of staffs contractual and statutory rights.</p> <p>For HR and business administration purposes.</p> <p>For defence against potential legal claims.</p>	<p>Legal Obligation.</p> <p>Performance of a contract or to enter into a contract.</p> <p>Legitimate Interests.</p>	<p>HR Consultants and Lawyers.</p>
<p>Financial and tax information (including pay and benefit entitlements, bank details and national insurance numbers).</p>	<p>To pay employees and make appropriate tax paymentsFor HR and business administration, and financial planning purposes. For defence against potential legal claims or safeguarding investigations.</p>	<p>Performance of a contract or to enter into a contract.</p> <p>Legal obligation.</p>	<p>Pension ProviderHMRCExternal benefits provider,HR Consultants and Lawyers.</p>
<p>Disciplinary and grievance records (including records of investigations, notes of disciplinary or grievance meetings and appeal hearings, correspondence with employees and written warnings).</p>	<p>To maintain a record of the operation of disciplinary and grievance procedures and their outcome.</p> <p>For HR and business administration purposes.</p> <p>For defence against potential legal claims or safeguarding investigations.</p>	<p>Legal Obligation.</p> <p>Legitimate Interests.</p>	<p>HR Consultants and Lawyers.</p>
<p>Absence and leave records containing special categories of Personal Data (including details of absence or leave taken, the reasons for absences, the type of leave, information about medical or health conditions, reasonable adjustments, records of absence management discussions, correspondence with employees and written warnings).</p>	<p>To maintain a record of the operation of absence procedures.</p> <p>To ensure that employees receive statutory and contractual sick pay or other pay entitlements (such as maternity or other family-related pay) and benefits.</p> <p>To meet health and safety obligations.</p> <p>To comply with the requirement to make reasonable adjustments.</p> <p>For HR and business administration purposes.</p> <p>For defence against potential legal claims or safeguarding investigations.</p>	<p>Performance of a contract or to enter into a Contract.</p> <p>Legal Obligation.</p> <p>Legitimate Interests Necessary to carry out obligations or exercise rights under employment law.</p>	<p>HR Consultants and Lawyers.</p>

Performance records (including appraisal documents, performance reviews and ratings, targets and objectives, performance improvement plans, records of performance improvement meetings and related correspondence, and warnings, work with students, safeguarding issues and concerns).	<p>To maintain a record of the operation of performance management systems and performance improvement processes</p> <p>For HR and business administration purposes</p> <p>For defence against potential legal claims or safeguarding investigations</p>	<p>Legal obligation.</p> <p>Legitimate Interests.</p>	HR Consultants and Lawyers.
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------	-----------------------------

### 20.3 Special Category Personal Data

The processing of the data relating to students and their relatives is restricted to what is necessary for the purposes of; carrying out and exercising the requirements of the contract between the Company and the Client of the Company's service, as is or may be required by law in the UK, to protect the vital interests of the Data Subject or others, in the course of the Company's legitimate activities with appropriate safeguards ensuring that special category data and Personal Data is not disclosed outside the Company unless required by law. All personal data is subject to the data protection measures of section 21, below.

### 20.4 Data Retention

The Company may retain information about any Data Subject, party to any Contract or referral for up to 85 years. However, information is only held for as long as necessary except as required by law, and for the Company's lawful business processing. The Company regularly reviews its records, to ensure that we only retain personal information for as long as necessary, for the purposes set out in this policy.

Where the Company no longer needs personal information, it will dispose of it, anonymise it, so that the Data Subject is no longer identifiable, or delete it in a secure manner without further notice to the Data Subject.

For unsuccessful applicants, or Education Specialists who's Contract ends before they have worked with a student, all data will usually be retained for 1 year.

## 21. DATA PROTECTION MEASURES

The Company subscribes to 'Cyber Essentials' and requires that all staff comply with its requirements when working with Personal Data, this includes:

- All emails containing Personal Data will be encrypted using secure data encryption for all electronic communication including attachments
- Where any Personal Data is to be erased or otherwise disposed of for any reason, including where copies have been made and are no longer needed, it will be securely deleted and disposed of. Hardcopies will be shredded, using a 'cross cut' shredder, and electronic copies should be deleted securely
- Personal Data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances
- Personal Data may not be transmitted over a wireless network if there is a wired alternative

that is reasonably practicable

- Personal Data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be archived. All temporary files associated therewith should be deleted
- Where Personal Data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data
- Where Personal Data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Royal Mail Special Delivery Service
- No Personal Data may be shared informally and if a member of staff requires access to any Personal Data that they do not already have access to, such access should be formally requested from the DPO
- All hardcopies of Personal Data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar
- No Personal Data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of the DPO
- Personal Data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time
- If Personal Data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it
- No Personal Data should be stored on any mobile device, including, but not limited to, laptops, tablets and smartphones, whether such device belongs to the Company or otherwise, without the formal written approval of the DPO and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary.

Where permission has been granted by the DPO to store personal information on a personal device the following must be adhered to:

- Data must never be accessed on a public computer
- If using a shared device, the user must have their own login, that no-one else has the password for
- All documents must be deleted and recycle bin emptied after they've been processed
- If using a mobile or tablet the company portal on Office 365 must be used to manage the device, so all personal data can be wiped remotely.

Unless agreed by a Director, no Personal Data should be transferred to any device belonging to staff, and Personal Data may only be transferred to devices belonging to staff where the parties in question have agreed to comply fully with the letter and spirit of this policy and of the Regulation, which may include demonstrating to the Company that all suitable technical and organisational measures have been taken.

All Personal Data stored electronically should be backed up at regular intervals with backups stored onsite and offsite. All backups should be encrypted using 256 bit encryption and or password protection.

All electronic copies of Personal Data should be stored securely using 256 bit data encryption and or password protection.

All passwords must contain a combination of uppercase and lowercase letters, numbers and symbols, and be a minimum of 8 characters. Software used by the Company is designed to require such passwords; safeguards are in place where this is not possible. The number of incorrect password attempts is limited 10 before an account is locked out, account login is restricted by location restriction, and where applicable multi-factor authentication and or the requirement for a VPN.

Under no circumstances should any passwords be written down or shared between staff irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords.

## **22. ORGANISATIONAL MEASURES**

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of Personal Data:

- All staff shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the Regulation and under this policy, and shall be provided with a copy of this policy
- Only staff that need access to, and use of, Personal Data in order to carry out their assigned duties correctly shall have access to Personal Data held by the Company
- All staff handling Personal Data will be appropriately trained to do so
- All staff handling Personal Data will be appropriately supervised
- Methods of collecting, holding and processing Personal Data shall be regularly evaluated and reviewed
- The performance of staff handling Personal Data shall be regularly evaluated and reviewed
- All staff handling Personal Data will be bound to do so in accordance with the principles of the Regulation and this policy by contract
- All staff handling Personal Data must ensure that any and all of their employees who are involved in the processing of Personal Data are held to the same conditions as those relevant employees of the Company arising out of this policy and the Regulation
- Where any staff member handling Personal Data fails in their obligations under this policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

## **23. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EUROPEAN ECONOMIC AREA**

The Company does not transfer Personal Data outside the European Economic Area.

## **24. DATA BREACH NOTIFICATION**

All Personal Data breaches must be reported immediately to the Company's DPO.

If a Personal Data breach occurs and that breach is likely to result in a risk to the rights and freedoms of Data Subjects, for example, financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage, the DPO must ensure that the Information Client's Office and the Data Subject is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

In the event that a Personal Data breach is likely to result in a high risk, that is, a higher risk than that described in the previous paragraph, to the rights and freedoms of Data Subjects, the DPO must ensure that all affected Data Subjects are informed of the breach directly and without undue delay.



Data breach notifications shall include the following information:

- The categories and approximate number of Data Subjects concerned
- The categories and approximate number of Personal Data records concerned
- The name and contact details of the Company's DPO or other contact point where more information can be obtained
- The likely consequences of the breach
- Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

### **Implementation of Policy**

This policy shall be deemed effective as of 1<sup>st</sup> August 2021. No part of this policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date. Previous copies of this policy are available on request.

This Policy has been approved and authorised by:

**Name:** Daniel Parrett  
**Position:** Operations Manager and Data Protection Officer  
**Date:** 8<sup>th</sup> August 2021  
**Due for Review by:** 8<sup>th</sup> August 2022  
**Signature:**



Created: August 2018  
Reviewed: August 2021  
Review date: August 2022