the supply register

Meeting the standards of APSCO Compliance+

Information Systems and Data Protection

Next to be reviewed: September 2026

We are the future of education recruitment.
We are The Supply Register.

1. Scope

This Data protection and processing Policy sets out how The Supply Register handle the Personal Data. This policy applies to all parties (employees, job candidates, customers, and suppliers etc. who provide any amount of information to us.

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the Company and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times.

The HR Department are responsible for overseeing this Data Processing Policy and, developing related policies and privacy policy.
Please contact the HR Department with any questions about the operation of this Data Processing Policy or the GDPR or if you have any concerns that this Data Processing Policy is not being or has not been followed.

2. Personal data protection principles

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

- Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency). Collected only for specified, explicit and legitimate purposes (Purpose Limitation).
  Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).
- Accurate and where necessary kept up to date (Accuracy).
- Kept in a form which permits identification of candidates for no longer than is necessary for the purposes for which the data is Processed (Storage Limitation).
- 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).
- Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).
- Made available to candidate's and they are allowed to exercise certain rights in relation to their Personal Data (Customers Rights and Requests).

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

3. Data protection

By signing your Statement of Terms and Conditions of Employment, you consent to the recording, processing, use, disclosure and transfer by the company of personal data relating to you.

You also give your consent to the company processing data relating to your sex and ethnic origin in order to monitor Equal Opportunities and data relating to your health in order to comply with Health & Safety legislation and for Human Resources management purposes.

This does not affect your rights to request copies of personal data of which you are the data subject, information about how the data is processed and the parties to whom the information may be disclosed under The Data Protection Acts (1984, 1998, 2000 and GDPR 2018).

At the sole discretion of the Managing Director, the company may, from time to time, carry out covert monitoring of activities, which the company cannot reasonably be expected to ignore. Such activities may include (but are not be limited to) criminal activity, gross misconduct, breaches of Health & Safety rules, or practices which jeopardise the safety of other employees.

Covert monitoring will not be embarked upon lightly and will only be sanctioned in cases where openness would prejudice an investigation and that the monitoring, taking account of its intrusiveness is a proportionate response to the mischief. The Managing Director will retain responsibility for ensuring that all monitoring is properly documented, and that the company retains full responsibility for data protection compliance.

4. Who is covered under the Data Protection policy?

Employees of our company and its subsidiaries must follow this policy. Contractors, consultants, partners and any other external entity are also covered. Generally, our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data. As part of our operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc.

Our company collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

Our data will be:

- Accurate and kept up-to-date
- Collected fairly and for lawful purposes only
- Processed by the company within its legal and moral boundaries
- Protected against any unauthorized or illegal access by internal or external parties

Our data will not be:

- Communicated informally
- Stored for more than a specified amount of time
- Transferred to organizations, states or countries that do not have adequate data protection policies
- Distributed to any party other than the ones agreed upon by the data’s owner (exempting legitimate requests from law enforcement authorities)

In addition to ways of handling the data the company has direct obligations towards people to whom the data belongs. Specifically, we must:

- Let people know which of their data is collected
- Inform people about how we’ll process their data Inform people about who has access to their information
- Have provisions in cases of lost, corrupted or compromised data
- Allow people to request that we modify, erase, reduce or correct data contained in our databases

5. Actions

- To exercise data protection we're committed to:
- Restrict and monitor access to sensitive data Develop transparent data collection procedures
- Train employees in online privacy and security measures
- Build secure networks to protect online data from cyberattacks
- Establish clear procedures for reporting privacy breaches or data misuse Include contract clauses or communicate statements on how we handle data
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.) Our data protection provisions will appear on our website.

6. Lawfulness and fairness

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the candidate. We will only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes.

These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the candidate. The GDPR allows Processing for specific purposes, some of which are set out below:

The candidate has given his or her Consent;
The Processing is necessary for the performance of a contract with the candidate; To meet our legal compliance obligations;
To protect the candidate's vital interests;

To pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of candidate's. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices.

7. Consent

Personal Data will only be processed on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

A candidate consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

You are easily able to withdraw Consent to Processing at any time and withdrawal will be promptly honoured. Consent may need to be refreshed if we intend to Process Personal Data for a different and incompatible purpose which was not disclosed when you first consented.

8. Transparency (Notifying you)

The GDPR requires Data Controllers to provide detailed, specific information to you depending on whether the information was collected directly from you or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain

language so that you can easily understand them. Whenever we collect Personal Data directly from you, we must provide you with all the information required by the GDPR including the identity of the Controller and DPO, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the candidate first provides the Personal Data. When Personal Data is collected indirectly (for example, from a third party or publicly available source), we will provide you with all the information required by the GDPR as soon as possible after collecting/receiving the data. We will also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

9. Purpose limitation

Personal Data will be collected only for specified, explicit and legitimate purposes. It will not be further processed in any manner incompatible with those purposes. We cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed you of the new purposes and you have consented where necessary.

10. Data minimisation

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

We may only Process Personal Data when performing our job duties requires. We cannot Process Personal Data for any reason unrelated to our job duties.

We may only collect Personal Data that we require for our job duties: do not collect excessive data. We ensure any Personal Data collected is adequate and relevant for the intended purposes.

We will ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

11. 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 use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it.

We will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards.

We will take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

12. Storage limitation

Personal Data will be kept in an identifiable form for no longer than is necessary for the purposes for which the data is processed.

We will not keep Personal Data in a form which permits the identification of you for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

We will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

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

13. Reporting a personal data breach

The GDPR requires Controllers to notify any Personal Data Breach to the applicable regulatory and, in certain instances, the candidate.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify you or any applicable regulator where we are legally required to do so.

14. Transfer limitation

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. We transfer Personal Data originating in one country across borders when we transmit, send, view or access that data in or to a different country.

We may only transfer Personal Data outside the EEA if one of the following conditions applies:

- The European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the candidate' rights and freedoms;
- Appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;
- The candidate has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the candidate, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the candidate where the candidate is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

15. Your right and requests

You have rights when it comes to how we handle your Personal Data. These include rights to:

- withdraw Consent to Processing at any time;
- receive certain information about the Data Controller's Processing activities;
- request access to your Personal Data that we hold;
- prevent our use of your Personal Data for direct marketing purposes;
- ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
- restrict Processing in specific circumstances;
- challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- object to decisions based solely on Automated Processing, including profiling (ADM);
- prevent Processing that is likely to cause damage or distress to the candidate or anyone else;
- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the supervisory authority; and
- In limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format. We will verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade us into disclosing Personal Data without proper authorisation).

16. Accountability

The Supply Register have appropriate technical and organisational measures in effect, to ensure compliance with the GDPR principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

The Company have adequate resources and controls in place to ensure and to document GDPR compliance including:

- Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of candidate;
- Integrating data protection into internal documents including this Data Processing Policy, Related Policies, Privacy Guidelines or Privacy Notices;
- Regular training Company Personnel on the GDPR, this Data Processing Policy, Related Policies and Privacy Guidelines and data protection matters including, for example, candidate's rights, consent, legal basis, DPIA and Personal Data Breaches.
- The Company maintain a record of training attendance by Company Personnel.
- Regularly test the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

17. Record keeping

The GDPR requires us to keep full and accurate records of all our data Processing activities. We will keep and maintain accurate corporate records reflecting our processing including records of candidate's consents and procedures for obtaining consent.

These records include, at a minimum clear descriptions of the Personal Data types, candidate types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to

create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

17. Training and audit

We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.
We will undergo all mandatory data privacy related training and ensure our team undergo similar mandatory training.

We will regularly review all the systems and processes under your control to ensure they comply with this Data Processing Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

18. Sharing personal data

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.
We may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

We may only share the Personal Data we hold with third parties, such as our service providers if:

- They have a need to know the information for the purposes of providing the contracted services; - Sharing the Personal Data complies with the Privacy Notice provided to the candidate and, if required, the candidate ‘s Consent has been obtained;
- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- The transfer complies with any applicable cross border transfer restrictions; and
- A fully executed written contract that contains GDPR approved third party clauses has been obtained.
- Government requests e.g. HMRC, DWP

19. Changes to this data processing policy

We reserve the right to change this Data Processing Policy at any time so please check back regularly to obtain the latest copy of this Data Processing Policy. We last revised this Data Processing Policy on 1st September 2025.

This Data Processing Policy does not override any applicable national data privacy laws and regulations in countries where the Company operates.