Aspire Recruitment Solutions Candidate/Recruiter/School Privacy Policy

Modified: 03/01/2023

It is the policy of Aspire Recruitment Solutions to respect the confidentiality of information and the privacy of individuals and organizations that engage in our services. This document describes the privacy policy for our educational staff recruitment services.
This policy explains how we collect personal information, the treatment of personal information that we collect when you are on our website, when you use our services, and use and disclosure of that information. This policy also applies to Aspire's treatment of any personal information.
This policy is provided to:

- Protect the security and confidentiality of protected information;

- Protect against anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of Protected Information that could result in substantial harm or inconvenience to any customer.

This policy also provides for mechanisms to:

- Identify and assess the risks that may threaten protected information maintained by Aspire;
- Designate employees responsible for coordinating the program;
- Design and implement a safeguards program;
- Manage the selection of appropriate service providers;
- Adjust the plan to reflect changes in technology, the sensitivity of protected information, and internal or external threats to information security; and
- Reference related policies, standards, and guidelines.

Identification and Assessment of Risks to Customer Information:
Aspire recognizes that it has both internal and external risks. These risks include, but are not limited to:

- Unauthorized access of protected information by someone other than the owner of the covered data and information
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system

- Corruption of data or systems
- Unauthorized access of covered data and information by employees
- Unauthorized requests for covered data and information
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of covered data and information through third parties.

Aspire recognizes that this may not be a complete list of the risks associated with the protection of protected information. Since technology growth is not static, new risks are created regularly. Accordingly, Aspire will actively monitor for new risks. Aspire believes the current safeguards in place are reasonable and are sufficient to provide security and confidentiality to protected information maintained by Aspire.

Control and Persistence of Your Private and Non-Private Data:
A two-year employment cycle is common at international schools. This includes the practice of us keeping Candidate data ready for touch-up and redeployment in the next employment cycle.
Pursuant to data privacy laws, you may have the right to have your information removed from our systems, entirely. You may do so by using our data privacy **form**.
Personal Information Collection: It is Aspire's usual practice to collect personal information directly from you through the use of CV's, Application forms and Aspires website in response to our printed and online advertisements.**Express Consent:** You acknowledge that if you submit an application, CV or contact our services, your application or request for services will constitute your express consent to our use of your personal information in accordance with our Privacy Policy as amended from time to time.
Information Types: Personal information that we collect, and hold is information that is reasonably necessary for the proper performance of our services and technology platforms. The information collected will differ depending on whether you are a school, a candidate, or a referee.

For Schools and School Recruiters: The type of information that we typically collect and hold about Schools and Recruiters is information that is necessary to help us manage the delivery of our services and support the function of our technology platforms and includes:

- Communication between Schools and Recruiters with Candidates;
- Communications between Schools and Recruiters with Aspire;
- Organizational contact and title information; and Billing and invoicing details.

For Candidates: The type of information that we typically collect and hold about Candidates is information that is necessary for Aspire Clients to assess Candidate's suitability for placements by our Clients or Client Organizations. Information includes:

- Contact details;
- Training and education details and history;
- Family details, including occupation of partner, ages of children, schooling requirements of children, housing requirements;
- Letters of recommendation;
- Communications between Candidates and Recruiters;
- Communications between Candidates and Aspire;
- Historical notes, and notes typical of customer service;
- Work history and relevant personal details
- Any criminal records; Employment preferences;
- Offer and placement information; Event registration and attendance;
- Candidate interests and preferences.

For Referees: The type of information that we typically collect and hold about Referees is information that is necessary to help to make determinations about the suitability of a Candidate by a Client and includes:

- Contact details and relevant work history;
- Record of comments provided; and Rankings of Candidates by Referees.
- Sensitive information is a special category of personal information. Aspire does not collect, and does not use sensitive information to influence how we present Candidates to prospective employers. Any unsolicited sensitive information that a Candidate shares, as part of a text held or otherwise, will not be used by Aspire for any discriminatory purpose.
- Sensitive Information is information or opinion about you, including but not limited to:
    - membership of a professional or trade association, or membership of a trade union;
    - health information;
    - political opinions,
    - philosophical views, membership of a political association;
    - religious beliefs or affiliations;
    - or sexual preferences or practices.

Aspire does encourage all parties to use a non-discriminatory hiring process that does not use race, gender, age, or sexual orientation to influence their hiring decisions.

Protected Information: Protected information shall include, but is not limited to, any of the following categories of information and data:

- A user name or e-mail address in combination with a password or security question and answer that would permit access to an online account; or
- “Personal information” in combination with any one or more of the following unencrypted data elements:
    - National Insurance number or QID;
    - driver’s license number or non-driver identification card number;
    - account number, credit or debit card number, in combination with a security code, access code, password or other information that would permit access to an individual’s financial account;
    - account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual’s financial account without additional identifying information, security code, access code, or password; or

“Personal information” shall mean “any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such person.”

Collection: The personal information that you submit to Aspire will be used internally, and for the benefit of other recruiting members of Aspire, who might require access to your personal information:

- when you complete any application forms or provide any other information in connection with the services you utilize with Aspire;
- via any of your references;

- as a result of inquiries that we might make of a professional association or registration body;
- as a result of any complaint or other information from or about you;
- via any information about any insurance investigation, litigation, registration or professional disciplinary matter, criminal matter, inquest or inquiry in which you were involved;
- or when you provide us with any additional information about you or your organization.

Photos and Images: We may also receive personal information from trusted third parties. We may ask to see scanned photographic ID, including a passport or other relevant documentation where we need to verify your identity, work rights or qualifications.

Use of Information and Information We Share: Aspire may use personal information collected depending on whether you are:

- a School Recruiter or a School Organization;
- a Candidate of Aspire ;
- or a Referee of a candidate.

For Schools and Recruiters of Aspire recruitment services, any personal information that we collect, hold, use and disclose about Clients is typically used to:

- assist your organization in finding qualified applicants;
- perform client and business relationship management;
- support the Aspire services that we deliver to you;
- facilitate Aspire marketing services to you;
- provide support of the function of our technology platforms;
- or support statistical purposes and statutory compliance requirements.

For Candidates of Aspire, information that we collect, hold, use and disclose about Candidates is typically used to:

- assist you in finding employment;
- assist you in being identified by a Recruiter via your searchable information;
- administer, protect and improve our website and our systems;
- better understand your website preferences;
- inform you about our services;
- respond to a request that you sent us.

For Referees of Aspire Candidates, information that we collect, hold, use and disclose about Referees is typically used for:

- confirm identity and authority to provide references;
- completing a candidate's suitability assessment;
- support of the function of our technology platforms;
- statistical purposes and statutory compliance requirements.

Direct Marketing: We may use information you provide us to contact you about our services that we believe may be of benefit to you. We will never sell your information to any third parties for marketing purposes. We comply with the requirements of anti-spam legislation and will give you the option of unsubscribing to email that is not essential to perform our intended business purpose.

How Personal Information is Stored: Personal information is held in our technology platforms until the time it is no longer needed for any purpose for which it may be used or disclosed. At this point it will be anonymized or destroyed, provided that it is lawful for us to do so.

We take a range of measures to protect your personal information from:

- misuse, interference and loss;
- and unauthorized access, modification or disclosure.

Information Security: We adopt a number of procedures to protect the information that we hold from unauthorized access, including but not limited to:

- Staff training;
- Password protection policy for all Aspire information technology services;
- Restricting access to information on a “need to know” basis;
- Policies and procedures to secure information on Aspire’s infrastructure including mobile devices such as laptops and smart phones;
- and Culling procedures including data deletion/data anonymizing, physical shredding and secure document disposal.

Information Transfer, Data Storage, and Hosting: All Aspire privacy data related to the technology services offered is hosted and managed by:Aspire. All data will be hosted by Aspire at Google: https://policies.google.com/privacy?hl=en-GB

Disclosure: Your personal information may be disclosed to employees, clients and licensees of Aspire and trusted third parties include those in countries that we provide services to, regarding possible work placements or to assist us in providing our services to you, professional associations or registration body that have a legitimate interest in the disclosure of your personal and sensitive information and any person with a lawful entitlement to obtain the information.

We will also send information about you to other companies or people when we:

- have your consent to share the information;
- need to share your information to provide the product or service you have requested;
- need to send the information to companies who work on behalf of Aspire to provide a product or service to you (unless we tell you

differently, these companies do not have any right to use the personal information we provide to them beyond what is necessary to assist us);

- respond to subpoenas, court orders or legal process; or
- find that your actions on our web sites violate the above terms of service, or any of our usage guidelines for specific products or services.

Failure to Provide Personal Information: If you do not give us the information we seek we may be limited in our ability to assist you.
Correction: Aspire may take such steps to make appropriate corrections, deletions and additions, in the circumstances that are reasonable to ensure that personal information is accurate, up to date and not misleading.
Access Policy: If you wish to obtain access to your personal information you should contact us and request the form to do so.
You will need to be in a position to verify your identity.
Control and Persistence of Your Private and Non Private Data:
Aspire operates their recruitment operations in a way that best supports the approximate 2-year employment cycle that is common at international schools. This includes the practice of us keeping Candidate data ready for touch-up and redeployment in the next employment cycle. For the Candidate's convenience, we will retain Candidate information for as long as eight years after the last time that they were an active member of Aspire recruitment services. Approximately at the start of each recruitment season, Aspire will securely dispose of any information that is beyond our retention policy, or that is no longer required. Where required by applicable law, we will notify you when such information has been disposed of.
Under the new guidelines of GDPR and other laws, you may have the right to be removed from our systems, entirely. You may initiate a request using our data privacy form.
Your Rights: You have the right to withdraw your consent at any time or to access and request that we rectify or remove your personal information from our system(s). Local laws may give you additional rights, such as the right to

request the information in your file, in a commonly readable format, at any time.

If you need assistance accessing, updating, correcting or removing your personal information from our System, or if you no longer desire our services, please request a **form**. Please note that we will request proof of identity prior to acting on any request. In certain circumstances (for example where required or permitted by law) we might not be able to provide you with access to some of your personal information, but where appropriate, we will notify you of the reasons for this.

Links: Please be aware that when using our website it may contain links to third-party websites. This Policy applies solely to information collected through the website. If you land on our website from other websites (or move to other sites from our website) you should read their separate privacy policies.

Cookies and Analytics: Cookies are text files containing small amounts of information which may be downloaded to your computer or mobile device when you visit a website. We use cookies and analytics tools to help deliver our online services, identify any service issues, improve our online services, provide content tailored to users' likely interests and personal preferences, send information to you by post, email or other means that we think may be of interest to you, and monitor site traffic and usage. We use some nonessential cookies and analytics on our website, such as Google Analytics to monitor and improve our efficacy and performance.

More information about the ways in which Google Analytics collects and processes personal data can be found here: https://policies.google.com/technologies/partner-sites.

More information about cookies, including how to block them on all sites or delete them, can be found at https://www.aboutcookies.org.

Design and Implementation of this Policy: Aspire is responsible for coordinating, maintaining and updating this Policy.

1. **Employee Management and Training**

During employee orientation, each new employee in departments that handle protected information will receive proper training on the importance of confidentiality of protected information. Each new employee will also be

trained in the proper use of computer information and passwords. Furthermore, each department responsible for maintaining protected information will provide ongoing updates to its staff. These training efforts should help minimize risk and safeguard covered data and information security.

2. **Physical Security**

Aspire addresses the physical security of protected information by limiting access to only those employees who have a business reason to know such information. Existing policies establish a procedure for the prompt reporting of the loss or theft of protected information. Offices and storage facilities that maintain Protected Information limit access and are appropriately secured. Protected information in electronic form that is no longer needed is securely erased so that the protected information cannot be read or reconstructed. Paper documents that contain protected information are shredded at time of disposal.

3. **Information Systems**

Information systems include network and software design, as well as information processing, storage, transmission, retrieval, and disposal. Aspire has policies, standards, and guidelines governing the use of electronic resources and firewall and wireless policies. Aspire will take reasonable and appropriate steps consistent with current technological developments to make sure that all protected information is secure and to safeguard the integrity of records in storage and transmission. Aspire will develop a plan to protect all electronic protected information by encrypting it for transit.

4. **Management of System Failures**

Aspire will maintain effective systems to prevent, detect, and respond to attacks, intrusions and other system failures. Such systems may include maintaining and implementing current anti-virus software; checking with software vendors and others to regularly obtain and install patches to correct software vulnerabilities; maintaining appropriate filtering or firewall technologies; alerting those with access to covered data of threats to security; imaging documents and shredding paper copies; backing up data regularly and storing back-up information off site, as well as other reasonable measures to protect the integrity and safety of information systems.

5. **Selection of Appropriate Service Providers**
Due to the specialized expertise needed to design, implement, and service new technologies, vendors may be needed to provide resources that Aspire determines not to provide on its own. In the process of choosing a service provider that will maintain or regularly access protected information, the evaluation process shall include the ability of the service provider to safeguard protected information. Contracts with service providers may include the following provisions:

- A stipulation that the protected information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- An assurance from the contract partner that the partner will protect the protected information it receives.

6. **Continuing Evaluation and Adjustment**
Aspire will regularly test and monitor the effectiveness of key controls, systems and procedures of this policy. This policy will be subject to periodic review and adjustment, especially when due to the constantly changing technology and evolving risks. Aspire will review the standards set forth in this policy and recommend updates and revisions as necessary. Accordingly, it may be necessary to adjust this policy to reflect changes in technology, the sensitivity of employee/customer data and internal or external threats to information security.

Questions and Complaints: You have a right to complain about our handling of your personal information if you believe that we have interfered with your privacy. Complaints can be initiated by requesting a form.
Complaints Procedure: If you are making a complaint about our handling of your personal information, it should first be made to us in writing using our **form**, or writing to Compliance:
Aspire Recruitment Solutions
18 Blake St, York,YO1 8QG,United Kingdom

Any information we hold will be governed by the most current version of the privacy policy.