

# Privacy Notice for Job Applicants

The Jo Richardson Community School (JRCS) is committed to protecting the privacy and security of your personal information. This privacy notice describes how we collect and use personal information about you during the application process in accordance with the General Data Protection Regulation (GDPR).

Successful candidates should refer to our 'Privacy Notice for Staff' for information about how their personal data is stored and collected.

## Who collects this information?

JRCS is a 'Data Controller' for the purposes of data protection law. This means that we are responsible for deciding how we hold and use personal information about applicants.

We are required under data protection legislation to notify you of the information contained in this privacy notice. This notice does not form part of any contract of employment or other contract to provide services and we may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

## Personal data that we collect, process, hold and share

We may collect, store and use the following categories of personal information about you up to the shortlisting stage of the recruitment process:

- Personal information and contact details such as name, title, addresses, date of birth, phone numbers and personal email addresses;
- Information collected during the recruitment process that we retain during your employment including proof of right to work in the UK, information entered on the application form, CV, qualifications;
- Details of your employment history including job titles, salary and working hours;
- Your racial or ethnic origin;
- Information regarding your criminal record as required by law to enable you to work with children;
- Information on conduct and/or other disciplinary issues involving you;
- Details of your referees and references;
- Images captured by the school's CCTV system.

We may also collect information after the shortlisting and interview stage in order to make a final decision on whom to recruit, including criminal record information, references and information regarding qualifications.

We may also ask about details of any conduct, grievance or performance issues, appraisals and timekeeping from references provided for you.

## Collecting this information

We may collect this information from you, your referees, your education provider, relevant professional bodies, the Home Office and from the Disclosure and Barring Service (DBS);

## How we use your personal information

We will only use your personal information when the law allows us to. Most commonly, we will use your information in the following circumstances:

- Where we need to take steps to enter into a contract with you;
- Where we need to comply with a legal obligation (such as health and safety legislation, under statutory codes of practice and employment protection legislation);
- Where it is needed in the public interest or for official purposes;
- Where it is necessary for our legitimate interests (or those of a third party) and your interests, rights and freedoms do not override those interests.

Generally, the purpose of us collecting your data is to enable us to facilitate safe recruitment and determine suitability for the role. We also collect data in order to carry out equal opportunities monitoring and to ensure appropriate access arrangements are put in place if required.

If you fail to provide certain information when requested, we may not be able to take the steps to enter into a contract with you (for example if incorrect references are provided), or we may be prevented from complying with our legal obligations (such as to determine suitability to work with children).

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

### **How we use particularly sensitive information**

Sensitive personal information (as defined under the GDPR as 'special category data') require higher levels of protection and further justification for collecting, storing and using this type of personal information. We may process this data in the following circumstances:

- In limited circumstances, with your explicit written consent;
- Where we need to carry out our legal obligations in line with our data protection policy;
- Where it is needed in the public interest, such as for equal opportunities monitoring;
- Where it is needed in relation to legal claims or where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent.

We will use this information in the following ways:

- To comply with employment and other laws;
- To facilitate safe recruitment and determine suitability for the role;
- Collecting information about your race or ethnic origin to ensure meaningful equal opportunity monitoring and reporting.

### **Criminal convictions**

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where it is necessary to carry out our legal obligations. We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.

Where appropriate, we will collect information about criminal convictions as part of the recruitment process in order to comply with safeguarding requirements.

### **Who we share your information with**

We may need to share your data with third parties, including third party service providers where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

These include the following:

- Academic or regulatory bodies to validate qualifications/experience (for example the Teaching Agency);
- Referees;
- Our Local Authority in order to meet our legal obligations for sharing data with it;
- Other schools;
- Disclosure and Barring Service (DBS); and
- Recruitment and supply agencies.

We may also need to share some of the above categories of personal information with other parties, such as HR consultants and professional advisers. Usually information will be anonymised but this may not always be possible. The recipients of the information will be bound by confidentiality obligations. We may also be required to share some personal information with our regulators or as required to comply with the law.

### **Retention periods**

Except as otherwise permitted or required by applicable law or regulation, the school only retains personal data for as long as necessary to fulfil the purposes they collected it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

How long we keep your information will depend on whether your application is successful and you become employed by us, the nature of the information concerned and the purposes for which it is processed.

The school typically retains job applicant personal data for six months from the date of interview, subject to any exceptional circumstances, or to comply with laws or regulations that require a specific retention period.

## **Security**

We have put in place measures to protect the security of your information (ie, against it being accidentally lost, used or accessed in an unauthorised way). In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know.

Third parties will only process your personal information on our instructions and where they have agreed to treat information confidentially and to keep it secure.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

## **The lawful basis on which we use this information**

We will only use your information when the law allows us to. Most commonly, we will use your information in the following circumstances:

- Consent: the individual has given clear consent to process their personal data for a specific purpose;
- Contract: the processing is necessary for a contract with the individual;
- Legal obligation: the processing is necessary to comply with the law (not including contractual obligations);
- Vital interests: the processing is necessary to protect someone's life;

We need all the categories of information in the list above primarily to allow us to comply with legal obligations. Please note that we may process information without knowledge or consent, where this is required or permitted by law.

## **Your right of access to your personal data**

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Under data protection legislation, you have the right to:

- Access your personal information (commonly known as a 'subject access request'). This allows you to receive a copy of the personal information we hold about you and to check we are lawfully processing it. You will not have to pay a fee to access your personal information;
- Correction of the personal information we hold about you. This enables you to have any inaccurate information we hold about you corrected;
- Erasure of your personal information. You can ask us to delete or remove personal data if there is no good reason for us continuing to process it;
- Restriction of processing your personal information. You can ask us to suspend processing personal information about you in certain circumstances, for example, if you want us to establish its accuracy before processing it;
- Object to processing in certain circumstances (for example for direct marketing purposes);
- Transfer your personal information to another party.

If you want to exercise any of the above rights, please email [gdpr@jorichardson.org.uk](mailto:gdpr@jorichardson.org.uk).

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

## **Right to withdraw consent**

In circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please email [gdpr@jorichardson.org.uk](mailto:gdpr@jorichardson.org.uk).

Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

## Contact us

If you would like to discuss anything within this privacy notice or have a concern about the way we are collecting or using your personal data, we request that you email [gdpr@jorichardson.org.uk](mailto:gdpr@jorichardson.org.uk) in the first instance to raise your concerns.

We have appointed a Data Protection Officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolved by emailing [gdpr@jorichardson.org.uk](mailto:gdpr@jorichardson.org.uk), then you can contact the DPO on the details below:

### ***Data Protection Officer (DPO)***

Name: Craig Stilwell

Details: Judicium Consulting Ltd, 72 Cannon Street, London, EC4N 6AE

Email: [dataservices@judicium.com](mailto:dataservices@judicium.com)

You have the right to make a complaint at any time to the Information Commissioner's Office, the UK supervisory authority for data protection issues at <https://ico.org.uk/concerns>.