

JOB APPLICANT PRIVACY NOTICE

Data controller: Stirling University Innovation Park Ltd

Designated Responsible Person: Lynn Harris, Head of Innovation Park (lynn.harris@suip.co.uk)



As part of any recruitment process, the company collects and processes personal data relating to job applicants. The company is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does the company collect?

The company collects a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number;
- details of your qualifications, skills, experience and employment history;
- information about your current level of remuneration, including benefit entitlements;
- whether or not you have a disability for which the company needs to make reasonable adjustments during the recruitment process; and
- information about your entitlement to work in the UK.

The company may collect this information in a variety of ways. For example, data might be contained in application forms, CVs or resumes, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment, including online tests.

The company may also collect personal data about you from third parties, such as references supplied by former employers. The company will seek information from third parties only once a job offer to you has been made and will inform you that it is doing so.

Data will be stored in a range of different places, including on your application record, in HR management systems and on other IT systems (including email).

Why does the company process personal data?

The company needs to process data to take steps at your request prior to entering into a contract with you. It may also need to process your data to enter into a contract with you.

In some cases, the company needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check a successful applicant's eligibility to work in the UK before employment starts.

The company has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows the company to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. The company may also need to process data from job applicants to respond to and defend against legal claims.

The company may process special categories of data, such as information about ethnic origin, sexual orientation or religion or belief, to monitor recruitment statistics. It may also collect information about whether or not applicants are disabled to make reasonable adjustments for candidates who have a disability. The company processes such information to carry out its obligations and exercise specific rights in relation to employment.

The company will not use your data for any purpose other than the recruitment exercise for which you have applied.

Who has access to data?

Your information may be shared internally for the purposes of the recruitment exercise. This includes members of the HR and recruitment team, interviewers involved in the recruitment process, managers in the business area with a vacancy and IT staff if access to the data is necessary for the performance of their roles.

The company will not share your data with third parties, unless your application for employment is successful and it makes you an offer of employment. The company may share your data with third parties engaged by the company to assist in the recruitment process. The company will then share your data with former employers to obtain references for you, employment background check providers to obtain necessary background checks to obtain necessary criminal records checks.

How does the company protect data?

The company takes the security of your data seriously. It has internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties.

We take the security of your data seriously and have controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by COMPANY employees such as those in HR, your Line Manager and/or the Directors in the performance of your duties. We restrict access to only those who need to so they can discharge their duties, restricting access to the HR and payroll folder on the server, by keeping hard copy files for HR and payroll purposes locked with access available only to the Head of Innovation Park and Head of Finance, and by storing all finance folders containing personal financial data such as bank details or P11D tax forms in a locked filing cabinet.

We have implemented data encryption on payroll reports following in and out of the company as well as any employee information on life insurance and pension.

In addition, we have deployed a number of systems to ensure your data remains safe, these include:

- A program of quarterly patch management, this ensures desktops and servers stay up to date with latest security patches.
- We use firewalls to protect our network borders, to stop our data being breached.

- All desktops run antivirus and anti-ransomware software.
- Taking regular backups.

Archived information is stored securely on-site.

Where we engage external companies to process personal data on our behalf, under a duty of confidentiality these organisations are also obliged to comply with the GDPR and implement appropriate technical and organisational measures to ensure the security of data. We have obtained statements of compliance and where appropriate amendments to contracts from all such third parties.

For how long does the company keep data?

If your application for employment is unsuccessful, the company will hold your data on file for 6 months after the end of the relevant recruitment process. At the end of that period your data is deleted or destroyed.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file and retained during your employment. The periods for which your data will be held will be provided to you in a new privacy notice.

Your rights

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the company to change incorrect or incomplete data;
- require the company to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing; and
- object to the processing of your data where the company is relying on its legitimate interests as the legal ground for processing.

If you believe that the company has not complied with your data protection rights, you can complain to the Information Commissioner.

What if I do not provide personal data?

You are under no statutory or contractual obligation to provide data to the company during the recruitment process. However, if you do not provide the information, the company may not be able to process your application properly or at all.

Automated decision-making

Recruitment processes are not based solely on automated decision-making or profiling.