Job Applicant Privacy Notice

HR&OD

1. Introduction

This notice explains how Human Resources and Development (HR & D) of Cranfield University ("the University", "we" and "our")) will collect and use, or otherwise process, the personal data relating to our job applicants ("you" and "your").

We are committed to ensuring that your personal data is handled in accordance with the principles set out in Data Protection legislation, as in force from time to time.

2. What information do we collect about you?

We collect and process your personal data for a number of purposes, including (but not limited to), records of:

- 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 University needs to make reasonable adjustments during the recruitment process;
- information about your entitlement to work in the UK to include details of any visa you hold and copies of passports;
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.
- results of any assessments and/or occupational testing;
- information on any clearances required, such as Disclosure and Barring Service (DBS) checks;
- information about medical or health conditions, provided at offer stage, including whether or not you have a disability for which the University needs to make reasonable adjustments.

The University may collect this information in a variety of ways. For example, data might be collected through application forms, CVs or resumes; obtained from your passport or other identity documents such as your driving licence; from correspondence with you; and from forms completed prior to employment; or collected through interviews or other forms of assessment.

The University may also collect personal data about you from third parties, such as references supplied by former employers, information from employment background check providers and information from criminal records checks. Normally the University 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).

3. Why does the University process personal data?

Processing of your personal data may be necessary for compliance with our legal obligations, or may be necessary in pursuit of our legitimate interests (where we have concluded that our interests do not impact inappropriately on your fundamental rights and freedoms). We have a legitimate

interest in fulfilling our duties and obligations, and managing our relationship with you during the recruitment process.

Processing data from our job applicants allows the University to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. For example:

- The University may process information about whether or not applicants are disabled to make reasonable adjustments for candidates who have a disability. This is to carry out its obligations and exercise specific rights in relation to employment.
- Where the University processes other special categories of data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is for equal opportunities monitoring purposes and provision of this data, is optional.
- For some roles, the University is obliged to seek information about criminal convictions and offences. Where the University seeks this information, it does so because it is necessary for it to carry out its obligations and exercise specific rights in relation to employment.

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

If your application is unsuccessful, the University may keep your personal data on file in case there are future employment opportunities for which you may be suited. The University will ask for your consent before it keeps your data for this purpose and you are free to withdraw your consent at any time.

4. Who has access to data?

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

The University will not share your data with third parties, unless your application for employment is successful and it makes you an offer of employment. The University will then share your data with former employers to obtain references for you, employment background check providers to obtain necessary background checks and the Disclosure and Barring Service to obtain necessary criminal records checks.

We may disclose certain personal data to external bodies in compliance with legal obligations. The amount of information provided to external bodies is limited to that which is permitted by Data Protection legislation.

Non-exhaustive examples of bodies to whom we are required by law to disclose data are:

Disclosure to	**Reason**
Home Office, UK Visas and Immigration	To fulfil the University's obligations as a visa sponsor
Verifile, the Disclosure and Barring Service (DBS) and National Security Vetting (NSV)	Required for certain sensitive posts to assess applicant's suitability for positions of trust or where the post works with vulnerable people or children.

We may also disclose certain personal data to external bodies where it is in our legitimate interests to do so, for example as part of our relationship with you, or for the purpose of aiding police and similar authorities in their investigations. We also have a legitimate interest in outsourcing data processing activities to third parties, where appropriate and in accordance with requirements of

Data Protection legislation. Again, the amount of information provided to external bodies is limited to that which is permitted by Data Protection legislation.

Non-exhaustive examples of information we may elect to disclose are set out in the table below.

Disclosure to	**Reason**
Agencies with responsibilities for the prevention and detection of crime, apprehension and prosecution of offenders, or collection of a tax or duty.	As necessary, and with appropriate consideration of your rights and freedoms
Occupational Health and our Employee Assistance Provider	To enable the provision of these facilities.
Third party data processors	To facilitate the activities of the University. Any transfer will be subject to an appropriate, formal agreement between the University and the processor.

5. Transferring information overseas

Your personal information may be transferred outside of the United Kingdom and where this occurs it will always take place under legitimate processing purposes and with the following controls.

For example, personal data may be processed by a third party provider, such as SHL's Talent Assessment Services, who state that a limited number of their personnel in the U.S. and India offices may also have access to Personal Information. Where this occurs, the transfer will be done on the basis that anyone to whom we pass it to protects it in the same way we would and in accordance with applicable laws.

Therefore, when we transfer your information to countries outside of the European Economic Area (which includes countries in the European Union as well as Iceland, Liechtenstein and Norway), we will only do so where:

a) the European Commission has decided that the country or the organisation we are sharing your information with will protect your information adequately;
b) the transfer has been authorised by the relevant data protection authority; and/or
c) we have entered into a contract with the organisation with which we are sharing your information (on terms approved by the European Commission) to ensure your information is adequately protected. If you wish to obtain a copy of the relevant data protection clauses, please contact the GDPR Team GDPR@cranfield.ac.uk

6. How does the University protect data?

The University 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.

7. For how long does the University keep data?

The University will keep your personal data only as long as is necessary to conclude the purpose(s), as set out above, for which it was collected. All data is held incompliance with Data Protection legislation, and in accordance with the University's Data Retention Schedule.

8. Automated decision-making

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

9. Your rights

You have the right: to ask us for access to, rectification or erasure of your data; to restrict processing (pending correction or deletion); to object to communications; and to ask for the transfer of your data electronically to a third party (data portability). Some of these rights are not automatic, and we reserve the right to discuss with you why we might not comply with a request from you to exercise them.

If you wish to make such a request, please write to:

University Data Protection Officer
Executive Office
Cranfield University
Cranfield
Bedfordshire
MK43 0AL

dataprotection@cranfield.ac.uk

You retain the right at all times to lodge a complaint about our management of your personal data with the Information Commissioner's Office at https://ico.org.uk/concerns/.

Document title	Job Applicant Privacy Policy
Document owner	Director of Human Resources and Development
Professional Service Unit/Department	Human Resources and Development Group
Implementation/effective date	May 2018
Approval by and date	Director of Human Resources and Development
Date of last review and version number	V2 - November 2019
Date of next review	December 2020
Title	Head of HR Compliance, Policy & Data

Document Review

Version	Amendment	By	Date
V1	GDPR compliant Job Applicant Privacy Notice	Head of HR Compliance, Policy and Data	May 2018
V2	Annual review undertaken – minor changes to the legislation footnote.	Information Security Manager/ Head of HR Compliance, Policy and Data	October 2019