



Data Protection Policy & Appropriate Policy Document

This policy is applicable to all members of Cranfield University that process personal data, including for example staff, students and contractors.

Background

Cranfield University's mission is to be an exclusively postgraduate university that is a global leader for education and transformational research in technology and management. In achieving this mission and, as part of its daily operations, the University takes the protection of the personal data it processes extremely seriously. The University will take reasonable and proportionate measures to ensure that it protects personal data against accidental or deliberate misuse, damage or destruction. It is also committed to a policy of protecting the rights and freedoms of all individuals, in relation to the processing of their personal data, in compliance with UK Data Protection legislation and EU General Data Protection Regulation where relevant.

Purpose

The purpose of this policy is to ensure that all members of the University comply with data protection legislation when processing personal data. Any serious infringement will be treated seriously by the University and may be considered under disciplinary procedures. A serious breach of the Data Protection Act may also result in the University and/or the individual being held liable in law.

Scope

The University processes personal information to enable us to provide education and support services to our students, professional learners, staff and alumni; manage our accounts and records; provide commercial activities to our clients; undertake research; advertise and promote the university and the services we offer; publish university and alumni publications and undertake fundraising. We also process personal information through surveillance camera systems that monitor and collect visual images for the purposes of research, security and the prevention and detection of crime.

This policy applies regardless of where the personal data is held or whether it is held manually or electronically.

Local conditions for processing

In addition to this policy, ensure you are aware of any local or specific conditions that are in place for the processing of personal data, e.g. when used for research purposes, and if in doubt speak to your Line Manager, tutor and/or School or Professional Service Unit Data Protection Champion in the first instance. Where necessary further clarification can be sought from gdpr@cranfield.ac.uk.

Principles

The University adheres to the principles of the UK Data Protection Act 2018. In accordance with these principles personal data (including special category and criminal offence data) shall be:

Data Protection Act 2018
Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
We have informed individuals what Cranfield will be doing with their data and why. and have identified an appropriate lawful basis for processing personal data and a schedule 1 condition for processing special category or criminal offence data.
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. We will only collect the data we need for the stated purpose.
Personal data shall be accurate and where necessary kept up to date.
Personal data shall be kept in a form, which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data is processed.
Personal data shall be processed in a manner that ensures appropriate security of the personal data including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organizational measures. We will keep personal data secure and limit access to those that need it.
As the data controller Cranfield University is responsible for the personal and special category data processed and able to demonstrate compliance with the data protection principles.

Roles and responsibilities

All

The University expects all its members to comply fully with its Data Protection Policy and the law.

Staff

Staff are responsible for:

- ensuring that all the personal data the University holds about them in connection with their employment is accurate and up to date.
- informing the University of any changes or errors to information which they have provided immediately, e.g., change of address either via Agresso or other appropriate channels, dependent upon the circumstances.

- ensuring, where they process personal data in connection with their employment and are permitted to do so under the University’s notification to the ICO, that any personal data processed is kept securely and is not disclosed orally, electronically or in written or image formats to any unauthorised third party.
- Ensuring that the data protection training is undertaken annually.
- informing GDPR (GDPR@cranfield.ac.uk) if they process personal data for a new purpose, transfer personal data to a new data processor or undertake any significant changes to the management or handling of personal data.

Where any of the above activities are to be undertaken a Data Protection Impact Assessment (DPIA) of this new, or additional processing, will be completed (in line with DPIA policy to ensure compliance with data legislation prior to the processing of the personal data. Contact GDPR@cranfield.ac.uk to complete a DPIA.

Anyone responsible for creating or maintaining web pages should note that University Policy and the provisions of data protection legislation will relate to any personal data about individuals that may be held on web pages or accessed via them.

Students

Students must ensure that any information they provide to the University is accurate and is kept up to date. If they find themselves in a position where they are processing personal data about staff or other students (e.g., as a student representative on a university committee, or as the secretary of a CSA Club or Society), then they must comply with University Policy and the law.

Any students at Cranfield University who handle or process personal data about individuals (names, contact details, financial details, course details, personal circumstances, beliefs etc.) in the course of their studies must be aware of the processing principles and how to apply them.

In certain circumstances, e.g., research data further data processing conditions may be relevant and further information is available from your tutor and/or department in the first instance. Further clarification can be sought from GDPR@cranfield.ac.uk.

Other

This category includes other stakeholders, contractors, visitors, etc. who provide personal data to the University or process personal data on behalf of the University (Council Members, External Examiners, etc.) which must also comply with University Policy and the law.

Data subjects’ rights

Under Data Protection legislation, data subjects have the following rights:

Individuals Rights
The right of access - you have the right to request the personal data we hold about you, free of charge in most cases.
The right to be forgotten - you have the right to request that we delete your data.
The right to data portability - you have the right to request that we supply a copy of your data in a commonly-used and machine-readable format for you to transfer your data to another

<p>service provider.</p>
<p>The right to be informed - you have the right to be informed about our processing of your data</p>
<p>The right of rectification - you have the right to request the correction of your personal data when incorrect, out of date or incomplete.</p>
<p>The right to restrict processing - individuals can request that their data is not used for processing. The individual's record can remain in place, but not be used. The right to restrict processing - you can request that your data is not used for processing. Your record can remain in place, but not be used.</p>
<p>The right to object - you have the right to stop the processing of your data for direct marketing purposes.</p> <p>Cranfield University offers its members, and visitors to our website the opportunity to subscribe (opt in) to a number of electronic communications. Individuals have the possibility at all times to tell us they no longer wish to subscribe to our electronic communication service (opt out). All e-communications sent from us will provide clear instructions on how to unsubscribe from each service.</p>
<p>You also have the right to object to the processing of your data where you believe a decision has been made about you by fully automated means, which has adversely affected you.</p>
<p>The right to be notified - you have the right to be notified, without undue delay, if there has been a data breach which is likely to result in a high risk to your rights and freedoms.</p>
<p>The right to complain - The University is committed to ensuring that any concerns are dealt with quickly and fairly, and with due concern for the individuals involved. However, the University recognises that individuals may continue to be dissatisfied. If you wish to complain about the University's processing of your personal data you are entitled to complain to the Data Protection Officer who will nominate a Senior Officer of the University, who has not been involved in the original enquiry, to deal with your complaint.</p> <p>Data Protection Officer, Cranfield University, Cranfield, Bedfordshire, MK43 0AL e: gdpr@cranfield.ac.uk t: +44 (0) 1234 754536</p> <p>You retain the right at all times to lodge a complaint about our management of your personal data with the supervisory authority, in the UK this is the Information Commissioner's Office</p>

(ICO). The ICO will expect you to complain to us first and give us an opportunity to resolve the matter before contacting them. The ICO contact details are given below.

Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF.

Web page <https://ico.org.uk/make-a-complaint/data-protection-complaints/>
Live chat service ico.org.uk/livechat
ICO helpline on +44 (0) 303 123 1113.

The University is committed to the management of such requests. The rights described above do not apply in every circumstance. Further guidance about exercising your rights is available from gdpr@cranfield.ac.uk.

Personal data in the public domain

Information that is already in the public domain is exempt from data legislation. This would include, for example, information on staff contained within externally circulated publications such as the research papers. Any individual who has good reason for wishing details in such publications to remain confidential should contact the University's Data Protection Officer at gdpr@cranfield.ac.uk.

Privacy statement

Where personal data is being initially collected (for example on a form) or used for a further purpose(s) then data subjects need to be informed how their personal data will be used by the University. See the GDPR intranet pages collecting data guidance.

Appropriate Policy Document

In addition to processing your personal data we also process special category data and data concerning criminal offences. This may include.

- protected characteristics as outlined in the Equality Act 2010 and other relevant legislation.
- occupational health records
- DBS records
- criminal convictions
- Biometric data collected through facial recognition cameras and other sensors for research and security purposes.

Conditions for processing special category and criminal offence data

We will only process such data in relation to you where the processing meets one or more of the conditions for processing such data, as set out in Data Protection legislation. For example,

- we have a number of employment law duties and obligations, which require us to process special category and criminal conviction data, including those relating to ensuring the fair treatment of employees, and maintaining a safe and secure working environment.

- where necessary, special category data will be processed for the purposes of preventive or occupational medicine, including in order to assess the working capacity of an employee.
- Certain processing may also be necessary including processing to enable the establishment, exercise or defence of legal claims, or for research and statistical purposes.
- We also request you to declare diversity data (protected characteristics) at the time of your application for a post and through equality monitoring exercises. Provision of this data, which is processed by us for statistical purposes, is optional.

A complete list of processing conditions we use is given below, for further details please see the [privacy policy](#) which also includes links to the staff and student privacy notices, or email GDPR@cranfield.ac.uk.

- Explicit consent
- Employment, social security and social protection law
- Vital Interests
- Not-for-profit bodies
- Made public by the data subject.
- Legal claims and judicial acts
- Public interest
- Health and social care
- Archiving, research and statistics

Procedures for ensuring compliance with the principles.

When processing special category or criminal offence data we adhere to the principles of the UK Data Protection Act 2018, as detailed earlier in this document.

Retention

When processing special category or criminal offence data, for the most part, data will be kept for a standard retention period of seven years in line with statute of limitations. There will be some exceptions to this, and data may be kept for a shorter or longer period than seven years. For example, employment applicant data will be kept for less time. Some data will be kept for more than seven years where there is a legal obligation to do so (e.g., pension information).

Grievance/Complaints procedure

Staff

<https://www.cranfield.ac.uk/about/governance-and-policies>

Students

See the student handbook for details

Further Information

- The GDPR intranet pages provide practical measures and actions to assist with the correct processing of personal data (which includes collecting recording or holding such data), and although the pages are not an exhaustive resource they provide pertinent advice and information for everyone.
- [Information Commissioner's website \(ICO\)](#)
- [ICO's Guide to GDPR](#)

Any queries concerning this policy can be raised with the University Data Protection Officer by email: gdpr@cranfield.ac.uk

Appendix A - Definitions

Data	In the terms of the Act, data are information relating to an individual where the structure of the data allows information about the individual to be readily accessed. The information may be held in manual form (e.g., as written notes relating to a person or as part of a manual filing system structured by name, address or other identifier) or in a form capable of being processed electronically.
Personal data	Personal data' means any information relating to an individual who can be identified, directly or indirectly from the information. (E.g., staff or student ID, name, address, payroll details and exam results).
Special Category data	Some of the personal data we process can be more sensitive in nature and therefore requires a higher level of protection. This means personal data about an individual's: <ul style="list-style-type: none"> • race. • ethnic origin. • political opinions. • religious or philosophical beliefs. • trade union membership. • genetic data. • biometric data (where this is used for identification purposes). • health data. • sex life; or • sexual orientation.
Criminal convictions/ Offences	Personal data can include information relating to criminal convictions and offences. This also requires a higher level of protection.
Data Controller	Means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. In this instance, the University is the data controller of the personal data processed and is registered with the Information Commissioners Office (ICO) under the number Z4690919 .
Data processor	In relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller. For example, a contracted and authorised external supplier of services who receives and processes personal data on the University's behalf is a data processor.
Data processing	Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including – <ol style="list-style-type: none"> (a) organisation, adaptation or alteration of the information or data, (b) retrieval, consultation or use of the information or data, (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or (d) alignment, combination, blocking, erasure or destruction of the information or data. The definition of processing is very wide, and it is difficult to think of anything an organisation might do with data that will not be processing.
Data subject	Means an individual who is the subject of personal data. Data subjects might include staff, students, alumni, job applicants, consultants, former employees, and staff of other institutions, members of University Council and members of the public. In other words, the data subject is the individual whom particular personal data is about. The Data Protection Act does not count as a data subject an individual who has died or who cannot be identified or distinguished from others.

Document control

Document title	Data Protection Policy
Originator name/document owner	University Data Protection Officer

Professional Service Unit/Department	Executive Office
Implementation/effective date	1 November 2017
Approval by and date	Information Assurance Committee July 2022
Minor administrative changes	15/11/2022
Date of next review	July 2024
Standards reference	Not applicable