Data Protection Policy incorporating Appropriate Policy Document

This policy is applicable to all members of Cranfield University that process personal data, including staff, students and contractors. The University expects all its members to comply fully with this Data Protection Policy and data protection legislation.

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 process personal data in line with data protection legislation and understand how to do so. Any 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

This policy applies regardless of where in the world the personal data is held or whether it is held in paper, other manual form or electronically.

The University processes personal information for a number of reasons including 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.

Local conditions for processing

In addition to this policy, all stakeholders are responsible for ensuring they are aware of any local or specific conditions that are in place for the processing of personal data, and if in doubt speak to your Line Manager, Tutor and/or School or Professional Service Unit Data Protection Champion.

Policy information for students, contractors and visitors

This category includes students and 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.) and must comply with this policy and data protection legislation. All these stakeholders are responsible for:

- Ensuring that all personal data the University holds about them is accurate and up to date.
- Informing the University of any changes or errors to the information which they have provided immediately.
- Ensuring when processing the personal of others (names, contact details, financial details, course details, personal circumstances, beliefs, etc) that they comply with this policy and data protection law. This includes when processing personal data in the course of studies, or as a student representative on a university committee, or as the secretary of a CSA Club or Society).
- In certain circumstances, e.g., when collecting research data further data processing conditions may be relevant and further information is available from the tutor and/or department in the first instance, and also on the links below.
    - Research data management Pages - (cranfield.ac.uk)
    - Research ethics and integrity https://intranet.cranfield.ac.uk/researchethics/Pages/default.aspx

Policy information for all Staff

All 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.
- Completing data protection training and information security training as required
- Ensuring when processing personal data they are aware of and respect the rights of individuals (see appendix 3) and will forward any rights requests received to gdpr@cranfield.ac.uk
- Ensuring, when processing personal data of others, they work in compliance with the principles of the data protection act (see appendix 2 for detail) by
    - Including a privacy statement when personal data is collected (see GDPR intranet pages)
    - Consulting with GDPR@cranfield.ac.uk if unsure of the legal basis for processing data
    - Not using data collected for one purpose for another purpose.
    - Collecting, sharing or processing the minimum amount of data for the purpose
    - Ensuring personal data they process is accurate and kept up to date.
    - Ensuring they only keep personal data as long as there is necessary purpose for doing so. The retention schedule (on the GDPR intranet pages) provides more details.
    - Ensuring at the end of the retention period, personal data is deleted or anonymised.
    - Protecting and ensuring the security of personal data they have access to. More detail is available in the Information Security intranet pages and Information Security policy.
    - Ensuring that personal data is only shared with others (internally and externally) when it is appropriate to do so (contact GDPR@cranfield.ac.uk for guidance
    - Ensuring when sharing personal data it is done so securely using encryption or password protection.
    - Checking before sharing personal data externally (for example, with a supplier or another company who is carrying out work for Cranfield), if a data protection agreement is needed in addition to the standard contract/agreement. The legal office can help with this.
    - Reporting any incident, or breach, involving the loss, incorrect sharing or other processing of personal data that does not comply with this policy to gdpr@cranfield.ac.uk
    - informing GDPR@cranfield.ac.uk before processing personal data for a new purpose, introducing a new system or undertaking any significant changes to the management or handling of personal data.

Policy Information for Line Managers

- Line managers are responsible for acting on any outstanding data protection or information security training for their staff.

Policy information for Senior Managers

- Senior managers must develop and encourage good data handling processes within their area.

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.

If you are unsure about any processing of personal data or have questions email gdpr@cranfield.ac.uk

Appropriate Policy Document

In addition to processing 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 .

a. Explicit consent
b. Employment, social security and social protection law
c. Vital Interests
d. Not-for-profit bodies
e. Made public by the data subject.
f. Legal claims and judicial acts
g. Public interest
h. Health and social care
i. 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, in most cases we keep personal data for a standard 7-year retention period consistent with typical government guidelines on record keeping. There are exceptions to this, and some data will be kept for a shorter or longer period. For example, employment applicant data will be kept for less time, while the categories of student name and qualification will be kept for the lifetime of the University. Some further data will be kept for more than seven years where there is a legal obligation to do so (e.g. pension information).

Personal data will be kept as long as there is necessary purpose for doing so, these purposes include.

- To carry out business or support functions e.g. to provide proof of qualification.
- Under contractual terms e.g. agreements with partners or funding organisations may require us to keep data for specific periods of time
- To demonstrate compliance with audit purposes or legislative requirements.

We carry out a regular review of all categories of data held and have in place processes for the removal of data. At the end of the retention period, personal data will either be deleted or anonymised.

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.
- Email GDPR@cranfield.ac.uk
- 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 1 - Definitions

Term	Definition
Personal data	Personal data is any information that can identify a living person (either directly or indirectly), including just a name or reference number. (E.g., staff or student ID, name, address, payroll details and exam results). Personal data can be in many forms including electronic, paper and other manual formats.
Special Category data	Some of the personal data we process can be more sensitive in nature and therefore requires, and receives, a higher level of protection. This means personal data about an individual's: • 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 and receives a higher level of protection.
Children's data	This also requires and receives a higher level of protection.
Data Controller	The data controller is the person or organisation who determines the purposes for processing personal data and how it is 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 numberZ4690919.
Data processor	The data processor is a person or organisation who processes the data on behalf of the data controller. This does not apply to individual employees but to organisations we work with. For example, an external supplier of services that process personal data, for example external printers, or suppliers of IT systems to Cranfield.
Data processing	Processing is anything which can be done with data. For example collecting, storing, retrieving, making available to others, printing, matching sorting comparing and destroying.
Data subject	The data subject is the individual whose data we are processing. 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.
Data Protection Impact Assessment (DPIA)	A DPIA is carried out to assess the risk of new processing so that safeguards can be put in place. Inform GDPR@cranfield.ac.uk before processing personal data for a new purpose, introducing a new system, or undertaking any significant changes to the management or handling of personal data so that a DPIA can be completed.
Legitimate Interest Assessment (LIA)	A LIA is an assessment carried out to assess the legal basis for processing where the University wishes to consider and balance our legitimate interests against those of the data subject.
Data Incident	A data protection is the loss, incorrect sharing or other processing of personal data that does not comply with this policy. If you make a mistake or become aware of a data incident inform gdpr@cranfield.ac.uk

Anonymisation	Data can be anonymised by the removal of personal data elements so that the individual can no longer be identified. Contact gdpr@cranfield.ac.uk for advice on achieving this.
Pseudonymisation	Pseudonymisation is a way of reducing risk and improving security. For example, you could remove an individual's name and other personal data from a list and replace it with a number. This could be a useful technique for sharing data more securely. Contact gdpr@cranfield.ac.uk for advice on achieving this.

Appendix 2 Data protection principles

The University processes personal data in accordance with the principles of data protection legislation. These are summarised below, if you have any questions, please contact GDPR@cranfield.ac.uk for advice.

Legal wording	Explanation/Summary
a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency')	We have informed individuals what Cranfield will be doing with their data and why. We have identified an appropriate lawful basis for processing personal data and a condition for processing special category or criminal offence data. .
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');	We will not use personal data which we collect for one purpose for another purpose.
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')	We will only collect the data we need which is relevant and proportionate for the stated purpose.
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');	We have processes in place to check the accuracy of data we collect or create. We have processes for keeping personal data up to date and accurate. Where we become aware that data is inaccurate or out of date, we will take reasonable steps to update or delete without delay. We understand there are some types of personal data e.g. statistical, historical or research data where it is not appropriate to keep it up to date.
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');	In most cases we keep personal data for a standard 7-year retention period consistent with typical government guidelines on record keeping. Personal data will be kept as long as there is necessary purpose for doing so. The Cranfield retention schedule provides more details. At the end of the retention period, personal data will either be deleted or anonymised.
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised	We keep data secure and limit access to it. We have put in place appropriate technical, physical and organisational procedures to

or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').	safeguard and secure the information we process about individuals. We have strict security standards, and all our staff are required to undertake data protection and information security training. We limit access to personal information to those employees, or third parties who have a business or legal need to access it. More information is available in the Information Security policy. All users of university information are responsible for protecting and ensuring the security of the information to which they have access. If a user believes that personal data has been lost/stolen or compromised, then this must be immediately reported to the IT Service Desk for assessment and investigation. Personal data must be collected and processed in accordance with UK data protection legislation, and any incident involving Confidential–Personal Data must be reported using the GDPR incident reporting form:
The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles. You must have appropriate measures and records in place to be able to demonstrate your compliance.	As the data controller Cranfield University is responsible for the personal and special category data processed. We have put in place the appropriate technical and organizational measures to meet (and demonstrate we are meeting) the requirements of accountability, these include. o implementing appropriate policies; o taking a 'data protection by design and default' approach o putting written contracts in place with organisations that process personal data on our behalf; o maintaining documentation of our processing activities; o implementing appropriate security measures; o recording and, where necessary, reporting personal data breaches; o appointing a data protection officer who can be contacted by gdpr@cranfield.ac.uk

Appendix 3 Individuals' rights

Under UK data protection law all individuals whose data we process have a number of rights regarding the personal data we process. Cranfield must ensure that the rights of individuals are met. Information is given below, please note that the rights described above do not apply in every circumstance. If you require further clarification, contact GDPR@cranfield.ac.uk.

If you receive a rights request, please forward to gdpr@cranfield.ac.uk. If you require further clarification, contact GDPR@cranfield.ac.uk.

The right to be informed.
You have the right to be informed about how we collect and use your personal data. This privacy policy provides detailed information. We are happy to provide more specific information on request.

The right of access (also known as Subject Access Request (SAR)).
You have the right to request the personal data we hold about you.

The right to rectification.
You have the right to request the correction of your personal data when incorrect, out of date or incomplete.

The right to erasure.
You have the right to request that we delete your data. However there may be circumstances where the law or our contractual obligations mean we need to keep some of your data.
The right to restrict processing.
In certain circumstances you have the right to request that we restrict the processing of your personal data, for example while we consider your request under the right to rectification.
.
The right to data portability.
You have the right to request that we supply a copy of your data, which you supplied to us, in a commonly used and machine-readable format for you to transfer your data to another service provider.

The right to object.
You have the right to stop the processing of your data for direct marketing purposes. We offer visitors to our website the opportunity to subscribe (opt in) to a number of electronic communications. You have the possibility at all times to tell us you no longer wish to subscribe to our electronic communication service (opt out). All marketing e-communications you receive from us will provide clear instructions on how to unsubscribe from each service.

In certain circumstances you also have the right to request that your data is not used for processing. Your record can remain in place, but not be used.

Rights related to automated decision-making including profiling.
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.

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.

The right to withdraw consent.
Occasionally we rely on your consent to process your contact details. This means you have the right to withdraw your consent, or to object to the processing of your personal data for this purpose at any time. If at any point you want to withdraw your consent, please email gdpr@cranfield.ac.uk.

The right to complain.
We are 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.
Data Protection Officer,
Cranfield University, College Road, Cranfield, Bedford, MK43 0AL
e: gdpr@cranfield.ac.uk
t: +44 (0) 1234 754536

The right to lodge a complaint with a supervisory authority.
You have the right 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 (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.
Address: 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.

FOI Requests
For information on handling FOI requests see the Freedom of Information (cranfield.ac.uk pages.

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 September 2023
Date of next review	July 2025