Data Protection Policy

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 (see Appendix for definition) of their personal data, in compliance with UK Data Protection legislation.

Purpose

The purpose of this policy is to ensure that all members of the University comply with the provisions of UK data legislation (i.e. the Data Protection Act 1998) when processing personal data. Any serious infringement of the Act 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 to undertake fundraising. We also process personal information through CCTV 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.

Principles

The University adheres to the principles of both the current UK Data Protection Act and the European General Data Protection Regulation. In accordance with these principles personal data shall be:

Data Protection Act 1998	General Data Protection Regulation 2016[1]
Processed fairly and lawfully	Processed lawfully, fairly and in a transparent manner in relation to individuals
Processed for specified purposes only	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
Adequate, relevant and not excessive	Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accurate and up to date	Accurate and, where necessary, kept up to date; whilst having regard to the purposes for which data is processed, every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay.
Not kept longer than necessary	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

[1] The GDPR becomes enforceable on the 25th May 2018 - http://ec.europa.eu/justice/data-protection/reform/index_en.htm

Processed in accordance with data subjects' rights	GDPR does not contain a specific principle relating to individuals' rights - these are specifically addressed in separate articles (see GDPR Chapter III - https://gdpr-info.eu/chapter-3/)
Processed and held securely	Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
Not transferred outside the countries of the European Economic Area with adequate protection	GDPR does not contain a specific principle relating to overseas transfers of personal data - these are specifically addressed in separate articles (see GDPR Chapter V - https://gdpr-info.eu/chapter-5/)

In addition the GDPR introduces an 'accountability' principle, this ensures that Data Controllers (the University) are responsible for, and can demonstrate and verify their compliance with personal data legislation.

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 either orally or in writing to any unauthorised third party;
- informing the Governance Officer (dataprotection@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, must be completed to ensure compliance with data legislation prior to the processing of the personal data.

As part of the DPIA staff need to provide full details of the type of personal data to be processed (i.e. financial details, contact details, etc.), who the subject of the data is (students, staff, the public, etc), why the data is being processed (marketing, staff administration, etc) and whether the intention is at any time to transfer the data to a third party external to the University who is not the subject of the data, including whether this is an international partner.

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 you are advised to speak to your tutor and/or department in the first instance. Further clarification can be sought from the Governance Officer at dataprotection@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 the Data Protection Act 1998 individuals have a right to inspect or request all personal information held about them. This can include, for example, the contents of student files, staff files, enrolment forms, lists of members of staff etc. 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.

These rights have been expanded under the General Data Protection Regulation and are referenced in the Data Protection Guidelines.

https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/

The University is committed to the management of such requests and any individual wishing to obtain personal information about themselves must contact the Governance Officer at dataprotection@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 dataprotection@cranfield.ac.uk.

Privacy statement

Where personal data is being initially collected or used for a further purpose(s) then data subjects need to be informed through a Privacy (also known as a Fair Processing) Notice, how their personal data will be used by the University.

ICO Guidance on Privacy Notices:
https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/
https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/

Grievance/Complaints procedure

Staff

https://www.cranfield.ac.uk/~/media/files/corporate_documents/cranfield-university-ordinances-part-b-staff-matters-changes-october-2015-(1).ashx?la=en

Students

https://intranet.cranfield.ac.uk/EducationServices/Senate%20Handbooks%20201617/complaints-students.pdf

Data Protection Guidelines

Further information and more detailed advice and guidance can be found in the University's Data Protection Guidelines:
https://intranet.cranfield.ac.uk/DataProtection/Public%20library/Data%20Protection%20Guidelines.pdf

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

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	University Executive; 7 November 2017
Date of next review	May 2018
Standards reference	Not applicable

Document Review

Version	Amendment	By	Date
1.0	Rebranding and amendments undertaken to ensure compliance with Jisc best practice and the General Data Protection Regulation	Deputy Data Protection Officer	
1.1	Amendments following comments from Data Protection Coordinators	Deputy Data Protection Officer	18th October 2017
1.2	Further amendments to satisfy HMG Supplier requirements	Deputy Data Protection Officer	2nd November 2017
1.3	Inclusion of DPIA link in document	Deputy Data Protection Officer	10th April 2018

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
Any data relating to a living individual (e.g. name, address, payroll details and exam results).

Sensitive Personal data
A subset of personal data that relate to a living person, recording such things as racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, criminal convictions, etc.

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 has registered its purposes of processing with the Information Commissioners Office (ICO) under the numbers **Z5670166** and **Z4690919**.

ICO Public Register:
https://ico.org.uk/esdwebpages/search

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 –

(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.

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 are processed whenever compiled, stored or otherwise in either manual or electronic form. Where sensitive personal data collection is necessary, the explicit consent of the individual may be required.