General Data Protection Regulation (GDPR) Readiness Statement

Updated May 2018

Cranfield University is a specialist postgraduate institution with a worldwide reputation for excellence and expertise in aerospace, defence and security, environment and agrifood, energy and power, management, manufacturing, transport systems, and water.

Compliance with GDPR is a strategic priority for the University, and we are actively working with our colleagues and external stakeholders to implement our GDPR programme over the coming months.

This includes:

- reviewing activities which involve processing personal data of our students, clients, employees, contractors and marketing contacts to determine whether any changes to the way we do this are required,
- implementing the changes, where necessary, and tracking progress,
- updating our training and awareness programmes,
- liaising with our suppliers as we update the contracts we have with them (see *Suppliers*).

Cranfield University has a Data Protection Officer who is co-ordinating the University's compliance with GDPR.

Record keeping

We have documented all the types of personal data we process and our legal basis for doing so under GDPR.

We recognise ourselves as the Controller of this information and take steps to ensure that it is processed in compliance with data protection laws.

We rely on obtaining the consent of the data subject only where no other ground for processing is available. Any such consent will be reviewed as part of our GDPR programme to ensure we are able to satisfy the new requirements.

Policies, guidance and training

Policies and guidance

We have revised our Data Protection Policy and all other applicable policies and associated guidance to reflect the new GDPR requirements.

All Cranfield University staff are required to handle data in accordance with our Data Protection Policy and associated policies issued by us in specific areas. The Data Protection Policy and Guidelines ensures that we handle information in accordance with legislative requirements and good practice to safeguard individuals' rights.

Our terms and conditions of employment require employees to comply with our policies and binds us to standards of professional confidentiality.

All staff are required to read and confirm their understanding of the Cranfield IT Users Policy. When revisions are made to policies, or new policies are introduced, we communicate this information to all staff through our various internal channels.

Training

All staff are required to complete data protection, GDPR and information security awareness training on an ongoing basis.

An internal GDPR awareness campaign was run in the lead-up to 25 May 2018. We will continue the momentum to ensure data protection is embedded in business as usual. Prior to May 2018, as part of the awareness campaign, all staff completed GDPR training and had access to specific guidance to help them understand how to apply the data protection principles to their work.

Suppliers

Due diligence is carried out on all of our suppliers, in accordance with our Purchasing Policy. This includes an assessment of their ability to securely process personal or commercial data on our behalf. Depending on the nature of the service or product, this can require compliance with relevant information security standards and/or completion of an information security and data protection questionnaire.

As part of our GDPR programme, we have identified all of the suppliers we use who process personal data on our behalf. We are in the process of updating the contracts we have with them to incorporate the provisions for processor contracts as required by Article 28 of the GDPR.

Information security

Information security and the protection of personal information is of paramount importance to Cranfield University, forming part of our culture and values.

We promote a positive security culture via ongoing awareness activities and regular review of our information security risk landscape by risk owners and the relevant internal bodies (e.g. Information Assurance Committee, Information Security Working Group), with a commitment to continual improvement.

The University has a wide range of technological and procedural measures in place to mitigate against the occurrence and impact of information security incidents, including accidental loss or destruction of, or damage to, personal information.

We operate a layered set of IT security related controls, such as robust password standards, access control protocols and encryption where appropriate. We have a ‘secure environment’ that is accredited to the UK Governments Cyber Essentials scheme. Physical security controls include security patrols, CCTV and role-based electronic access cards. All server rooms have additional access controls with further limited access assigned or key pad with codes.

Role-based access controls (RBAC) are used to restrict access to electronic resources on Cranfield University systems.

Location and retention of data

Data is stored in electronic files, which are stored, backed up and supported within the UK. Some hard copy documentation will also be stored in physical files.

Data is retained in accordance with our Retention Policy, which specifies a standard retention period of seven years. We have defined categories of data where a longer retention period is required, such as pension, visa, research and qualification data. We have established a destruction process of logical or physical files at the end of the retention period. As part of our GDPR programme, we are working with all areas of the business to refine our Electronic Records Retention Policy.

Sub-contracting and data transfers

On occasion, it is necessary for us to transfer data overseas. If this is outside of the European Economic Area (EEA), we will take steps to ensure that personal data is adequately protected in accordance with UK legal requirements. Where we are in a contractual relationship with the recipient, such protection will normally consist, at minimum, of appropriate contractual protections agreed between us and the recipient (processor) of the data.

We will review and update existing guidance on how to manage international transfers as part of our GDPR programme.

To ensure that we deliver an exceptional level of service to our stakeholders (clients, students and staff, etc), we choose to outsource some of our services or engage consultants and others to support us (for example external examiners, IT services and support, marketing, courier or data improvement services).

Where we have such arrangements, relevant personal data would be provided to, and processed by, the provider of such services, in accordance with the terms of our contract with them and to the extent appropriate for the performance of that contract. These arrangements are being reviewed and formal contractual mechanisms appropriate to the recipient will be introduced as part of our GDPR programme.

Privacy by design and privacy impact assessments

When purchasing or developing new products and services, we carry out risk assessments of data protection and information issues. We are currently incorporating the principles of ‘privacy by design’ as a default into our project management and change control processes to ensure compliance with GDPR requirements.

Data incidents and breaches

We have reviewed our established process for handling data breaches. The revised process ensures that, when required, we are able to meet the new reporting obligations under GDPR. For example, we would notify the data subject of a breach as soon as is practically possible where this breach is likely to result in a high risk to their rights and freedoms.

Individuals’ rights

We have reviewed our established internal processes for managing individuals’ rights requests in light of the expanded rights of data subjects under GDPR and the reduced timeframe for complying with such requests.

Summary of the actions taken

Subject access requests (SAR)

- Cranfield staff and contractors are required to handle data in accordance with our Data Protection Policy, Data Protection Guidelines and other applicable policies, including ‘best practice communications’ i.e. how to recognise and report a SAR.

Information Security Policy and best practice

- We have communicated this to our staff, including how to recognise and report a SAR.

Additional rights under GDPR

- As part of our GDPR programme, we are working to identify personal data within our IT environment and define any changes necessary to ensure GDPR compliance in respect of individuals’ rights, such as the ‘right to be erased’ and ‘the right to portability’, as applicable.
- Processes and procedures have been designed to facilitate an efficient GDPR-compliant, ‘rights outcome’ delivery customer experience.