Anglia Ruskin University (ARU) Corporate Data Protection Policy

The University takes its data protection responsibilities seriously and seeks at all times to protect the rights and freedoms of individuals by processing their personal data securely in accordance with legal requirements.

The University holds personal data about students, applicants, staff, suppliers and other individuals for legitimate business purposes.

This Policy sets out how the University will protect personal data and ensure that staff understand their responsibilities when processing personal data. In particular this Policy requires that staff contact the Data Protection Officer before any new significant processing of personal data takes place, thereby ensuring compliance obligations are met.

Scope

This Policy applies to all individuals who work for the University and those providing services. The Policy is also applicable to all organisations who provide services to the University that involve the processing of personal data.

The Policy will be supported by various guidance materials, standard operating procedures and work instructions issued from time to time. Any such documentation will be circulated through normal communication channels.

Policy responsibility

The Data Protection Officer has overall responsibility for the Policy, and may be contacted for further advice via our website.

GDPR Principles

The University shall comply with the General Data Protection Regulation (GDPR) Principles, which are:

1. The collection of personal data must be lawful fair and transparent
2. Personal data is processed for specified purposes
3. Only the minimum necessary personal data is processed
4. Personal data must be accurate and up to date
5. Personal data cannot be stored any longer than necessary
6. The personal data must be kept safe and secure

GDPR accountability and transparency

The University must ensure transparency and accountability in relation to its use of personal data. This is accomplished by issuing a Privacy Policy and Privacy Notices so that individuals understand our processing of personal data. In addition we must document our data processing activities. This task is overseen by the GDPR Action Party (GAP), which is chaired by the Head of Risk & Compliance. The Secretary and Clerk, has overall responsibility for GDPR implementation and GAP will report to that post as Chair of the Data Governance Steering Committee (DGSC). All staff have responsibility for the personal data that they process.

Data Protection Impact Assessments (DPIA)

Any new processing must be notified to the Data Protection Office (DPO) who will assist staff to complete a DPIA where required. By conducting DPIAs we will ensure that we introduce all appropriate technical and organisational controls thereby implementing measures that provide privacy by design and by default including data minimisation, pseudonymisation and anonymisation where appropriate. This will ensure that we enhance security and privacy procedures as part of our business as usual approach. DPIA documentation and other GDPR tools are available at My.Anglia.

Fair and lawful processing

Processing of personal data must only be undertaken where we have a lawful basis for processing. Individuals have the right for any data to be deleted, if it is not lawfully processed. A correctly drafted Privacy Notice is essential.

Lawful basis for processing personal data

One of the following conditions must apply for processing personal data: a) consent; b) contract; c) legal obligation; d) Vital interests; e) public function; and f) legitimate interest.

Deciding on the lawful basis for processing

The processing must be necessary and you should establish which lawful basis is the most appropriate for the purpose. The lawful basis for processing should be the one that is expected by the individual. For the processing to be fair and lawful you must have informed the individual of the lawful basis for processing. For further advice contact dpo@anglia.ac.uk or see My.Anglia for information.

Special categories of personal data

These were previously known as sensitive personal data and consist of the following:
a) race; b) ethnic origin; c) politics; d) religion; e) trade union membership; f) genetics; g) biometrics (when used for ID purposes); h) health; and i) sexual orientation. Explicit consent is normally required but there are exemptions. Please see My.Anglia for further information, or contact dpo@anglia.ac.uk for further advice.

University's GDPR Responsibilities

Anglia Ruskin has a number of responsibilities under GDPR, including but not limited to:

- Provide a Privacy Notice at the point of data collection.
- Identify the lawful basis for processing.
- Ensure staff are trained appropriately.
- Provide a secure environment for the processing of personal data.
- Document and maintain records of data processing activities.
- Detect, report and investigate personal data incidents.

Individuals privacy rights

An individual has the right to request of the university the following: a) right of rectification; b) right to erasure; c) right to restriction of processing; d) right of data portability; e) right to object and f) automated decision making or profiling. If you should receive a request exercising one of these rights please see My.Anglia or contact dpo@anglia.ac.uk.

Privacy Notices

The University has a corporate approach to Privacy Notices. Please contact dpo@anglia.ac.uk for advice.

Using third parties - contracts

If you use a third party in relation to the processing of personal data then you must have a contractual relationship. For advice on GDPR contract clauses please see My.Anglia , or contact dpo@anglia.ac.uk

Incident reporting

The University holds the personal data of thousands of staff, students, alumni, research participants and others who have an association with the University. If that data is lost, stolen, corrupted or released to unauthorised persons, the Secretary & Clerks Office must be informed immediately, using the procedure and form available at My.Anglia.

The Management of ARU is committed to the success of the Corporate Data Protection Policy and will ensure that it is understood and implemented by all staff through adherence to all relevant supporting policies, procedures and guidelines as well as awareness training.

This Policy is reviewed annually by the ARU Corporate Management Team

Date of last review 27th April 2018