UNIVERSITY POLICY

Policy Name:	Data Protection Policy	**Policy ref. #**	SCO001
Approval Authority:	Corporate Management Team	**Original Adoption:**	30/04/2018
Responsible Dean / Director:	Paul Bogle	**Responsible Business Area:**	Office of the Secretary & Clerk
Contact:	David Humphreys, Information Compliance Team, dpa@anglia.ac.uk		
Review Frequency:	3 years	**Review Due:**	30/4/2020

Revision History

Policy revisions should not be made without stakeholder consultation and approval by appropriate authority

Date	Summary of Changes	Version
12/3/2020	• Including additional information required by Data Protection Act 2018 relating to processing of Special Category Data. This document now acts as the 'Appropriate Policy'. • Version 1 described implementation activities reflecting compliance status in 2018. Version 2 describes post-implementation 'business as usual'.	2

Table of Contents

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.

The General Data Protection Regulation (2016) and The Data Protection Act (2018) require organisations who process personal data to have in place appropriate security measures to protect personal data (GDPR Article 5.1(f)), document compliance with the principle of Accountability (Article 5.2) and maintain an 'appropriate policy' for the processing of Special Category Data (DPA Schedule 1, Part 4). Failure to do so risks regulatory action.

All employees and third party employees processing ARU personal data to support their understanding of their legal obligations, and to be made available to all ARU data subjects for transparency purposes.

4. **The Policy**

This Policy applies to all individuals directly employed by the University. The Policy is also applicable to employees of all organisations who provide services to the University that involve the processing of personal data for which ARU is a Data Controller. It also applies to University employees and suppliers if the University acts as a Data Processor and where a Data Controller accepts the provisions of this Policy as supporting its 'documented instructions'.

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

Policy responsibility

The Data Protection Officer has overall responsibility for the Policy, and may be contacted for further advice at dpa@anglia.ac.uk.

The GDPR Principles

The University complies with the General Data Protection Regulation (GDPR) Principles (Article 5, GDPR), which are:

1. *Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.*

   The University:
   - ensures that personal data is only processed where a GDPR Article 6 legal condition applies (and an Article 9 condition applies (supported by a DPA Schedule 1 condition where necessary) for Special Category Data), or a relevant DPA Schedule 2 exemption applies.
   - only processes personal data fairly, and will ensure that data subjects are not misled about the purposes of any processing. The University will consult Data Subjects where appropriate in order to inform a 'fairness' test.
   - ensures that data subjects receive full privacy information so that any processing of personal data is transparent; maintaining a Privacy Policy which provides this (and supporting detailed Privacy Notices where relevant).

2. *Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.*

   The University:
   - only collects personal data for specified, explicit and legitimate purposes, and we will inform data subjects what those purposes are through our Privacy Policy and supporting notices.
   - does not use personal data for purposes that are incompatible with the purposes for which it was collected, unless the law permits this. If we do use personal data for a new purpose that is compatible and it is not disproportionate to do so, we will inform the data subject first.
   - assesses the compatibility of re-use for research purposes through the Research Ethics Approval process.

3. *Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.*

   - The University only processes personal data if it is necessary to achieve its legitimate purposes.
   - The University collects the minimum personal data that is necessary to achieve the purpose for which it is collected. We ensure that the data we collect is adequate and relevant.

4. *Personal data shall be accurate and, where necessary, kept up to date.*

   - The University ensures that personal data is accurate. We take particular care to do this where our use of the personal data has a significant impact on individuals.
   - Personal data is kept up to date where this is necessary for the purpose for which it is collected.

5. *Personal data shall be 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.*

   The University:
   - only keeps personal data in identifiable form as long as is necessary for the purposes for which it is collected, or where we have an ongoing legal obligation to do so. Once it is no longer necessary to retain personal data it shall be securely deleted or rendered permanently anonymous.
   - maintains a Records Retention Policy and associated retention schedules, and that record will set out, where possible, the envisaged time limits for erasure of the different categories of data processed.
   - retains the minimum personal data necessary to evidence that records were appropriately deleted under the Records Retention Policy.
   - provides data subjects with full privacy information about how their data will be handled, and that this will include (or reference the schedules which contain) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.
   - retains personal data indefinitely for research and archiving purposes subject to appropriate security measures to safeguard data subject rights and freedoms

6. *Personal data shall be 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.*

   - The University ensures that there are appropriate organisational and technical measures in place to protect personal data.
   - Those measures are subject to frequent risk assessment taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.
   - The University complies with recognised security standards where these are relevant to the processing, meet with the University's strategic aims or are required as part of a contractual commitment, or statutory or regulatory requirement.
   - The University operates a process managing instances of breaches of security which lead (or could have lead) to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to,

personal data. The process appropriately assesses whether a breach meets the criteria for notification to the supervisory authority. The University's Staff Disciplinary Policy and Procedure may apply to breaches of this Policy by employees, the Rules, Regulations and Procedures for Students for Student breaches, and contractual provisions for Supplier breaches.

- The University safeguards the security of personal data and data subject privacy rights by making international transfers of personal data only where an appropriate GDPR Chapter 5 provision is in place.

7. *The University will be responsible for, and be able to demonstrate compliance with Principles 1-6.*

- All staff have responsibility for the personal data that they process and they shall be supported in their duties by:
    - Identifying and appropriately training key roles with specific responsibilities to oversee compliance with Data Protection legislation,
    - making available appropriate policy and guidance,
    - providing mandatory induction training and refresher training at a frequency appropriate to roles,
    - providing periodic awareness raising communications, campaigns and events.
- Procedure and guidance on aspects of Data Processing form part of this Policy and breaches of these associated controls are a breach of this Policy.
- The Secretary & Clerk has overall responsibility for Data Protection compliance, Chairs the Data Governance Steering Committee (DGSC), is a member of the Corporate Management Team (CMT) *and acts as Senior Information Risk Owner (SIRO).*
- A Data Protection Officer (DPO) provides advice on compliance, and acts as a contact point for the supervisory authority on issues relating to the University's processing.
- Data Champions provide advice and support to the Faculty or Service which they represent and attend the Information Compliance Group (ICG) with the DPO, chaired by the Head of Risk & Compliance and reporting to DGSC.
- The University maintains a Record of Processing Activity available on request to the supervisory authority.
- The University's procurement, technology change and project management processes include privacy by design requirements to ensure that all processing is appropriately assessed for compliance with Data Protection law and the need to conduct Data Protection Impact Assessment where the envisioned processing meets the statutory criteria.
- All Contracts and Agreements governing relationships with partners and suppliers which involve the transfer of personal data or where a party processes personal data on behalf of another party contain provisions required by law governing the processing.
- Where an appropriate Code of Conduct or Accreditation scheme is mandated or is otherwise deemed relevant in whole or in part to the University's processing, the University will achieve and maintain compliance as required and will develop appropriate means of evidencing compliance.

Privacy Rights

The University operates appropriate processes by which a data subject (or their authorised representative) may exercise their Privacy rights under GDPR such as the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restriction of processing, the right to data portability, the right to

object and rights regarding automated decision-making including profiling. These rights may be exercised by contacting the designated contact details relating to services being received or by contacting dpa@anglia.ac.uk

5. **Resources**

Information for the public
Information for employees

6. **Definitions**

Term	Definition
Data Controller	A body which, alone or jointly with others, determines the purposes and means of processing personal data. (GDPR Art.4(7)).
Data Processor	A body which processes personal data on behalf of a controller (GDPR Art.4(8)).
Data Subject	An identified or identifiable natural living person to whom personal data relates (GDPR Art.4(1)).
International Transfer	The sharing of personal data with an organisation based in a country outside of the European Economic Area
Personal Data	Information which, directly or indirectly, identifies a data subject in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (GDPR Art.4(1)).
Processing	any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. (GDPR Art.4(2)).
Record of Processing Activities	A comprehensive record of all purposes of processing; a description of all categories of data subjects and of all the categories of personal data processed; the categories of recipients to whom personal data is disclosed and the retention period; a general description of technical and organisational security measures (GDPR Art.30(1)).
Special Category Data	Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. Processing of genetic data, biometric data for the purpose of uniquely identifying a data subject. Data concerning health or data concerning a data subject's sex life or sexual orientation (GDPR Art.9(1)).