Aston University

Data Protection Policy

May 2018

This document sets out the policy governing the University's policy governing the management and use of personal data

May 2018

Reference Number	Version Letter	Executive Sponsor	Officer Responsible for Policy/ Procedures	Consultation Process	Date of Approval and Committee and/or Executive Officer	Effective Date
LSP001/1718	1	Chief Financial Officer	Head of Legal Services	GDPR Working Party	Executive Operations Group Executive Committee	24 May 2018

Title

Data Protection Policy

Introduction and Context

Everyone has rights with regard to the way in which their personal data is handled. During the course of the University's activities it collects, stores and processes personal data about its students, staff, partners, suppliers and other third parties. The University recognises that the correct and lawful treatment of this data will maintain confidence in the University's compliance and will provide for successful business operations. This document sets out the Policy governing the University's collection, use and storage of personal data.

1. SCOPE OF THE POLICY

1.1 Purpose of the Policy

The purpose of this Policy is to ensure the correct and lawful treatment of personal data held by the University in accordance with data protection law and particularly the General Data Protection Regulation (EU) 2016/679 (GDPR).

1.2 What is covered by the Policy

This Policy sets out:

- *the basis on which we will process personal data we collect from data subjects, or that is provided to us by data subjects or other sources; and*
- *the rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.*

1.3 Who is covered by the Policy

All those who access personal data held by the University, including staff, must be aware of and comply with the Policy.

Staff are required to complete the University's mandatory training to inform them about personal data law so they will have an appreciation and understanding of the importance of compliance with this Policy. This policy does not form part of any employee's contract of employment and may be amended at any time.

1.4 Breach of this Policy

Any breach of this Policy and its associated procedures by staff will be investigated in accordance with the University's disciplinary procedure. A serious breach may amount to gross misconduct, and could therefore result in summary dismissal.

Any breach of this Policy and its associated procedures by non-staff will be investigated and steps taken in accordance with the law and any relevant contract.

1.5 Policy Ownership

The Executive has approved this Policy, the Chief Financial Officer is the Executive sponsor and the Head of Legal Services is the officer responsible for the Policy. Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the Head of Legal Services. The Head of Legal Services is the University's statutory Data Protection Officer in accordance with the requirements of the GDPR.

2. THE POLICY STATEMENT

2.1 Guiding Principles

The guiding principles of this Policy are aligned to the six data protection principles set out in data protection law and are to ensure that the University will:

- *process personal data lawfully in a fair and transparent manner;*
- *only collect and use personal data for specified, explicit, and legitimate purposes;*
- *minimise its use of personal data;*
- *ensure that personal data is accurate and kept up-to-date and corrected or deleted without delay when inaccurate;*
- *keep personal data in an identifiable form only for as long as necessary to fulfil the purposes for which the University collected it;*
- *keep personal data secure using appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction, or damage by maximising the use of electronic data systems;*
- *maintain and destroy its records in a manner that allows it to manage its legal risks and comply with the law; and*
- *ensure all staff are suitably of aware of their responsibilities under data protection law and will maintain expert resources to provide the necessary instructions and advice to staff.*

2.2 The Data Protection Procedures

Six Data Protection Procedures implement this Policy:

- *Data Subject Access Request Procedure;*
- *Data Correction Procedure;*
- *Data Erasure Procedure;*
- *Data Processing Restriction Procedure;*
- *Data Portability Procedure, and*
- *Data Breach Notification Procedure.*

3. DEFINITION OF DATA PROTECTION TERMS

The terms set out in this section 3 apply to this Policy.

Data is information which is stored electronically, on a computer, or in paper-based filing systems.

Data subjects for the purpose of this Policy include all living individuals about whom the University holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with data protection law. The University is the data controller of all personal data used within in it for its operational and business purposes.

Data users are those University employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this Policy and any applicable data security procedures at all times.

Data processors include any person or organisation that processes personal data on the University's behalf and on its instructions. University staff are excluded from this definition but it could include suppliers which handle personal data on the University's behalf.

Privacy notices are used by the University, as required by law, to provide data subjects with certain information about its data processing activities and must be concise, transparent, intelligible, easily accessible and expressed in clear and straightforward language. The University can provide privacy notices in writing, electronically if appropriate and orally in some cases.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. It can also include genetic and biometric data. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

4. DATA PROTECTION PRINCIPLES

By law, the University must comply with the six principles when processing personal data:

Lawfulness, fairness, and transparency.

Purpose limitation, which means that the University should only collect personal data for specified, explicit, and legitimate purposes and should not process the personal data in a manner that is incompatible with those purposes, except under limited circumstances.

Data minimisation, which means that personal data should be adequate; relevant; and limited to what is necessary for the purpose of processing.

Accuracy, which means that personal data must be accurate and kept up-to-date; and corrected or deleted without delay when inaccurate.

Storage limitation, which requires that the University keep personal data in identifiable form only for as long as necessary to fulfil the purposes the University collected it for, subject to limited exceptions. Please refer the Records Management Policy and its associated procedures for further guidance.

Integrity and confidentiality, which requires that the organisation secure personal data by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction, or damage. Please refer to the Information Security Policy for further guidance.

5. ACCOUNTABILITY AND DEMONSTRATING COMPLIANCE

By law, the University must demonstrate compliance with all six of the principles. This requires the establishment of this Policy and its associated procedures as well as the Records Management Policy and Procedures.

The University takes the following steps to ensure that it can further demonstrate its compliance by:

- determining and documenting a lawful basis for each instance of processing personal data;
- maintaining a record of data processing activities;

- providing data subjects with legally-compliant privacy notices and maintaining copies of privacy notices to demonstrate the University's authority to process the personal data;
- satisfying specific requirements when relying on data subject consent;
- satisfying specific requirements when processing sensitive personal data;
- honouring data subject rights, including rights relating to automated decision making and profiling; and
- complying with cross-border data transfer restrictions and maintaining compliant data transfer mechanisms.

6. DATA SUBJECT RIGHTS

By law, data subjects have certain rights.

The **right to confirm whether the University processes personal data about the data subject and the right to access the personal data processed** and obtain certain information about the processing activities. Please refer to the Data Subject Access Request Procedure for further guidance.

The **right to correct** inaccurate personal data. Please refer to the Data Correction Procedure for further guidance.

The **right to have personal data erased** under certain circumstances. Please refer to the Data Erasure Procedure for further guidance.

The **right to restrict the processing of personal data** under certain circumstances. Please refer to the Data Processing Restriction Procedure for further guidance.

The **right to receive a copy of the personal data the University holds** under certain circumstances and transfer the personal data to another data controller. Please refer to the Data Portability Procedure for further guidance.

The **right to object to processing** that is undertaken for the performance of a task in the public interest, for the purposes of the University or a third party pursuing its legitimate interests, direct marketing purposes or undertaken for scientific or historical research purposes or statistical purposes under certain circumstances.

The **right not to be subject to a decision based solely on automated data processing**, including profiling, where the decision has a legal or other significant effect, subject to certain limited exceptions, including where the data subject explicitly consents, where the automated data processing and decision-making is necessary for the performance of a contract with the data subject or where an applicable law that also requires measures to protect data subjects' rights authorises the automated data processing and decision-making.

The **right to a privacy notice** containing certain information about the processing activities. Data subject consent is one of several legal bases for processing personal data under law and the University uses its privacy notices to ensure it obtains valid consents as required. Certain requirements must be satisfied when relying on consent to process personal data, including a requirement that the University demonstrate that it obtained the data subject's consent.

The law requires that consent be:
- freely given, specific, and informed;
- unambiguous and take the form of an affirmative action or statement;
- explicit for certain types of data processing, including, but not limited to, sensitive personal data processing and cross-border data transfers;
- presented in a manner clearly distinguishable from other matters, in an intelligible and easily accessible form; and
- provided in clear and plain language.

When the University collects personal data from a child under the age of 13, it is required by law to obtain consent from the child's parent/legal guardian and take reasonable steps to verify that the parent/legal guardian consented.

The University also must notify each recipient of personal data, for example, third-party data processors, of any correction or erasure requests or restrictions on processing so that the third party can carry out the request.

7. DATA TRANSFERS

Data controllers and data processors transferring personal data outside of the EU must comply with certain legal requirements for those data transfers. Therefore, the University must ensure appropriate safeguards are in place. This may include usage of Standard Model Clauses or the requirement of explicit consent from data subjects. Please refer to Legal Services for further guidance.

8. JOINT CONTROLLERS

Where two or more data controllers determine the purposes and means of data processing, they are known as joint controllers.

When the University acts as a joint controller, it must:

- determine which data controller is responsible for certain obligations under law; and
- specify their duties by a written agreement which should include a point of contact for data subjects, reflect the data controllers' roles vis-à-vis the data subjects, be made available to data subjects and allow data subjects to exercise their rights against each of the data controllers.

9. DATA PROCESSORS

The law establishes specific obligations and requirements for engaging data processors. It only permits transfers to data processors when the data processor provides sufficient guarantees that it has implemented appropriate technical and organisational measures to protect personal data in accordance with the law.

The University's data processor relationships must be governed by a contract or other legal act under applicable law that binds the data processor. Furthermore, the data processor must have written authorisation from the University before engaging another data processor.

10. DATA BREACHES

The law requires the University to notify the Information Commissioner's Office without undue delay and no later than 72 hours after any breach of personal data that poses a risk of harm has been discovered. The University must also document any personal data breaches. Please refer to the Data Breach Notification Procedure for further guidance.