Data Protection Policy

Introduction

Amity University [IN] London ("the University") is committed to data protection by default and by design and supports the data protection rights of all those with whom it works, including, but not limited to, staff, students, visitors, alumni and research participants. This policy sets out the University's approach to data protection and information security, the accountability and responsibilities of the University, its staff and its students to comply fully with the provisions of the General Data Protection Regulation ("the GDPR") and the Data Protection Act 2018 ("the DPA") and it recognises that handling personal data appropriately and in compliance with data protection legislation enhances trust, is the right thing to do and protects the University's relationship with all its stakeholders.

The University holds and processes personal data about individuals such as employees, students, graduates and others, defined as 'data subjects' by the law. Such data must only be processed in accordance with the GDPR and the DPA.

The Compliance Officer monitors and advises on compliance with the GDPR and the DPA. However, responsibility for compliance and the consequences of any breaches cannot legally be transferred to the Compliance Officer but instead remains with the business area. Information and advice can be obtained from the Compliance Officer.

Purpose of Policy

This policy sets out the responsibilities of the University, its staff and its students to comply fully with the provisions of GDPR and the DPA. This policy forms the framework which everybody processing personal data should follow to ensure compliance with data protection legislation.

Scope

This policy applies to all staff and students in all cases where Amity University [IN] London is the data controller or a data processor of personal data. The policy applies in these cases regardless of who created the data, where it is held, or the ownership of the equipment used.

Status of the Policy

The policy has been approved by the Amity Executive Team on 8 May 2018. This policy does not form part of the formal contract between the University and staff or students, but compliance with it is a condition of employment and of the Student Contract to abide by the University's rules and policies. Any failure to follow the policy can therefore result in disciplinary proceedings.

Part One: Processing Data in accordance with the law

This section of the Policy explains the personal data that the University processes and how it does so in accordance with the principles which it is required to follow to ensure compliance with the law.

The University's Data Processing Activities

The University's **core data processing activities** are those necessary for:

- the registration, monitoring supervision, teaching, assessment and examination of its students and research participants
- the maintenance of relationships with past students, alumni and other academic institutions and
- the marketing and promotion of the University's reputation and services.

The purpose of this is to enable the University to undertake its primary functions as an educational establishment.

The University's **ancillary data processing activities** are those necessary for the management and administration of employees and independent contractors and related activities.

The purpose of this is to enable the University to employ and manage staff and to administer its undertaking in support of its primary function of providing educational services.

The University processes the following categories of Special Personal Data:

- racial and ethnic origin
- religious and philosophical beliefs and
- Employee Data.

Data Protection Principles

The GDPR sets out seven key principles ("the Principles") which lie at the heart of the general data protection regime

These are that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) 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 ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) 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 ('storage limitation');

(f) 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 ('integrity and confidentiality').

In addition (g), 'the accountability principle' requires the data processor shall take responsibility for what it does with personal data and how it complies with the other principles.

It is a legal requirement that the data controller shall be responsible for, and be able to demonstrate compliance with these principles.

Lawfulness, Fairness and Transparency

Lawfulness

In order to meet the 'lawfulness' requirement, processing personal data must meet at least one the following conditions:

1. The data subject has given consent.
2. The processing is required due to a contract.
3. It is necessary due to a legal obligation.
4. It is necessary to protect someone's vital interests (i.e. life or death situation).
5. It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
6. It is necessary for the legitimate interests of the controller or a third party.

We have identified the following appropriate lawful basis (or bases) for our core and ancillary processing activities:

When processing data in accordance with its core data processing activities, the University relies primarily on Conditions 1 and 2 above.

When processing data in accordance with its ancillary data processing activities, the University relies primarily on Conditions 1, 2 and 3 above.

Certain types of information is designated as special categories of personal data.

These are:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for the purpose of uniquely identifying a natural person.
- Health
- Sex life and sexual orientation

For special categories of personal data, at least one of the following conditions must be met:

1. The data subject has given explicit consent.
2. The processing is necessary for the purposes of employment, social security and social protection law.
3. The processing is necessary to protect someone's vital interests.
4. The processing is carried out by a not-for-profit body.
5. The processing is manifestly made public by the data subject
6. The processing is necessary for legal claims
7. The processing is necessary for reasons of substantial public interest.
8. The processing is necessary for the purposes of medicine, the provision of health or social care or treatment or the management of health or social care systems and services.
9. The processing is necessary for public health
10. The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to certain safeguards which are explained in the Handbook

The University will not carry out automated decision-making (including profiling) based on any individual's sensitive personal information.

We have identified the following appropriate lawful basis (or bases) for our processing of special categories of data: Conditions 1 and 2 above.

Fairness

In order to meet the 'fairness' requirement, we consider how our data processing may affect the individuals concerned and we have regard to what people would reasonably expect in the handling of their personal data. We also consider how we have obtained the data and how the way we process it affects the interests of the people concerned – as a group and individually. We do not use it in ways that have unjustified adverse effects on them. If the processing involves a detriment to an individual or individuals, we consider whether this detriment is justified.

Transparency

With regard to transparency, the university processes data in an open and honest way and we are clear at all times with all individuals for who we process data as to how we do this and what it will be used for.

Purpose Limitation

The purposes for which the University processes data have been identified (see The University's Data Processing activities above). This information is included in our privacy information for individuals. We will regularly review our processing and, where necessary, update our documentation and our privacy information for individuals. If at any time, the University intends to process data for a new purpose, we will check that this is compatible with our original purpose or we get specific consent for the new purpose.

Data Minimisation

We only collect personal data we actually need for our specified purposes. This means identifying the minimum amount of data that we require to fulfill our purposes and not holding any more than that. We periodically review the data we hold, and delete anything we don't need.

Accuracy

The University has appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data. We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary.

Mistake

If we need to keep a record of a mistake, we clearly identify it as a mistake.

Matters of opinion

Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts.

Right to rectification

We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data. As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data.

Storage Limitation

The University carefully considers and can justify how long we keep personal data. We have a policy with standard retention periods where possible.

This applies to all personal data, whether held on core systems, local PCs, laptops or mobile devices or held on paper. If the data is no longer required, it must be securely destroyed or deleted. The University's Retention Schedule is based on both legal and business requirements.

We regularly review our information and erase or anonymise personal data when we no longer need it. See the University's statement of Anonymisation of Personal Data.

We have appropriate processes in place to comply with individuals' requests for erasure under 'the right to be forgotten'.

Integrity and Confidentiality (Security)

The University undertakes an analysis of the risks presented by our processing, and use this to assess the appropriate level of security we need to put in place. When deciding what measures to implement, we take account of the state of the art and costs of implementation.

Data Security Policy

Please see the University's Data Security Policy. We take steps to ensure that this policy is implemented,

Additional Policies

Where necessary, we have additional policies and ensure that controls are in place to enforce them. Please see Policy on taking sensitive information and personal data outside the secure computing environment and Computing Regulations.

We make sure that we regularly review our information security policies and measures and, where necessary, improve them.

Technical Controls

We have in place appropriate technical controls and procedures to ensure the management and security of the data. We keep these under review and make changes as and when necessary.

Accountability and Governance

The University takes responsibility for complying with the Data Protection law, at the highest management level and throughout our organisation. We keep evidence of the steps we take to comply with this.

We put in place appropriate technical and organisational measures, such as those listed below.

We review and update our accountability measures at appropriate intervals.

Part Two: Technical and Organisational Measures

In addition to the policies and measures referred to above, the University has adopted the following measures and procedures

Privacy Notices

When the University collects personal data from individuals, the requirement for 'fairness and transparency' must be adhered to. This means that the University must provide data subjects with a 'privacy notice' to let them know how and for what purpose their personal data are processed. Any data processing must be consistent or compatible with that purpose. (Please see The Right to be Informed below0.

Data Protection Impact Assessment

Where data processing is likely to result in a high risk to an individual's data protection rights (for example, if the University is considering new processing activities or setting up new procedures or systems that involve personal data), privacy issues must always be considered at the earliest stage and a Data Protection Impact Assessment (DPIA) must be conducted. The DPIA is a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce risks during the design stages of a process and throughout the lifecycle of the initiative. This will ensure that privacy and data protection control requirements are not an after-thought.

A template and guidance for DPIAs can be found on Amity Moodle or through the Compliance Officer.

Anonymisation and Pseudonymisation

Further mechanisms of reducing risks associated with handling personal data are to apply anonymization or pseudonymisation. Wherever possible, personal data must be anonymised or, where that is not possible, pseudonymised.

Guidance on anonymization and pseudonymisation can be found on Amity Moodle or through the Compliance Officer.

Handling Research Data

Before commencing any research which will involve obtaining or using personal data and special categories of personal data, the researcher must give proper consideration to this policy. The researcher must ensure that the fairness, transparency and lawfulness principle is complied with and that privacy by design and default is applied. This means that wherever feasible, research data must be anonymised or pseudonymised at the earliest possible time.

Handling of Research Data by Students

The use of personal data by students is governed by the following:

- Where a student collects and processes personal data in order to pursue a course of study with the University, and this course of study is not part of a University-led project, the student rather than the University is the data controller for the personal data used in the research. If the data are extracted from a database already held by the University, the University remains the data controller for the database, but the student will be the data controller for the extracted data.

- Once a thesis containing personal data is submitted for assessment, the University becomes data controller for that personal data.
- Where a research student processes personal data whilst working on a project led by a University research group, the University is the data controller.

Academic and academic-related staff must ensure that students they supervise are aware of the following:

- A student should only use personal data for a University-related purpose with the knowledge and express consent of an appropriate member of academic staff (normally, for a postgraduate, this would be the supervisor, and for an undergraduate the person responsible for teaching the relevant class/course).
- The use of University-related personal data by students should be limited to the minimum consistent with the achievement of academic objectives. Wherever possible data should be anonymised so that students are not able to identify the subject.

Part Three: Data Subject Rights

The GDPR and the Act contain eight data subject rights the University must comply with . These are; The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making

The Right to be Informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. The University must provide individuals with information including: the purposes for processing their personal data, the retention periods for that personal data, and who it will be shared with. We call this 'privacy information'. We must provide privacy information to individuals at the time you collect their personal data from them. If the University obtains personal data from other sources, we must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month. The information you provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.

The Right to Access

Individuals have the right to request to see or receive copies of any information the University holds about them, and in certain circumstances to have that data provided in a structured, commonly used and machine readable format so it can be forwarded to another data controller. The University must respond to these requests within four weeks. It is a personal criminal offence to delete relevant personal data after a subject access request has been received.

Individuals receiving a subject access request must follow the subject access request procedures available on the University's website.

The rights to erasure, to restrict processing, to rectification and to object

In certain circumstances data subjects have the right to have their data erased. This only applies

- where the data is no longer required for the purpose for which it was originally collected, or
- where the data subject withdraws consent, or
- where the data is being processed unlawfully.

In some circumstances, data subjects may not wish to have their data erased but rather have any further processing restricted.

If personal data is inaccurate, data subjects have the right to require the University to rectify inaccuracies. In some circumstances, if personal data are incomplete, the data subject can also require the controller to complete the data, or to record a supplementary statement.

Data subjects have the right to object to specific types of processing such as processing for direct marketing, research or statistical purposes. The data subject needs to demonstrate grounds for objecting to the processing relating to their particular situation except in the case of direct marketing where it is an absolute right.

Individuals receiving any of these requests should not act to respond but instead should contact the Compliance Officer immediately.

Rights in relation to automated decision making and profiling

In the case of automated decision making and profiling that may have significant effects on data subjects, they have the right to either have the decision reviewed by a human being or to not be subject to this type of decision making at all. These requests must be forwarded to the Data Protection Officer immediately.

Part Four: Data Sharing

When personal data is transferred internally, the recipient must only process the data in a manner consistent with the original purpose for which the data was collected. If personal data is shared internally for a new and different purpose, a new privacy notice will need to be provided to the students.

When personal data is transferred externally, a legal basis must be determined and a data sharing agreement between the University and the third party must be signed, unless disclosure is required by law, such as certain requests from the Department for Work and Pensions or Inland Revenue, or the third party requires the data for law enforcement purposes.

Transfers of Personal Data outside the EEA

Personal data can only be transferred out of the European Economic Area when there are safeguards in place to ensure an adequate level of protection for the data. For transfers of personal data to a receiving party in the United States of America, the Privacy Shield Agreement between the European Union and the United States of America provides sufficient protection. Before transferring data, the Privacy Shield website should be consulted to determine whether the receiving party is on the Privacy Shield List. Staff involved in transferring personal data to other countries must ensure that an appropriate safeguard is in place before agreeing to any such transfer.

Direct Marketing

Direct marketing does not only cover the communication of material about the sale of products and services to individuals, but also the promotion of aims and ideals. For the University, this will include notifications about events, fundraising, selling goods or services. Marketing covers all forms of communications, such as contact by post, fax, telephone and electronic messages, whereby the use of electronic means such as emails and text messaging is governed by the Privacy and Electronic Communications Regulations 2003. The University must ensure that it always complies with relevant legislation every time it undertakes direct marketing and must cease all direct marketing activities if an individual requests it to stop.

Part Five: Responsibilities under the Policy

The University as data controller has a corporate responsibility to implement and comply with data protection legislation. Thus, in determining the purposes for which, and the manner in which, personal data is processed, the University must adhere to the seven Data Protection Principles set out in the legislation.

Data Security

All users of personal data within the University must ensure that personal data are always held securely and are not disclosed to any unauthorised third party either accidentally, negligently or intentionally. The Information Security Policy, the Policy on Taking Sensitive Information and Personal Data outside the Secure Computing Environment and the Computing Regulations must be read in conjunction with this Data Protection Policy. These documents are available on Amity Moodle or through the Compliance Officer.

Responsibilities of Management and Data Users

Heads of Units have a responsibility to ensure compliance with the GDPR, the DPA and this policy, and to develop and encourage good information handling practices within their areas of responsibility. All users of personal data within the University have a responsibility to ensure that they process the data in accordance with the Principles and the other conditions set down in the legislation. The Compliance Officer will perform periodic audits to ensure compliance with this policy and the legislation.

Data Protection Training

The Amity Executive Team agreed on 9 April 2018 that it should be mandatory for all staff members to complete the Data Protection Training. In addition, all academic members of staff must complete the training on Research under the GDPR.

Part Six: Data Protection Breaches

The University is responsible for ensuring appropriate and proportionate security for the personal data that it holds. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage of the data. The University makes every effort to avoid data protection incidents, however, it is possible that mistakes will occur on occasions. Examples of personal data incidents might occur through:

- Loss or theft of data or equipment
- Ineffective access controls allowing unauthorised use
- Equipment failure
- Unauthorised disclosure (e.g. email sent to the incorrect recipient)
- Human error
- Hacking attack

Any data protection incident must be brought to the attention of the Compliance Officer who will investigate and decide if the incident constitutes a data protection breach. If a reportable data protection breach occurs, the University is required to notify the Information Commissioner's Office as soon as possible, and not later than 72 hours after becoming aware of it. Any member of the University community who encounters something they believe may be a data protection incident must report it immediately to the Compliance Officer on ext 188 or riley@london.amity.edu.

Part Seven: Documentation and Records

The University will maintain records as required by the GDPR such as processing purposes, data sharing and retention. These records must be made available to the Information Commissioner's Office on request.