Data Protection Policy

1. Introduction

1.1 The University of Gloucestershire (the 'University') collects, holds and processes data about its students, employees, applicants, alumni, stakeholders, contractors and other individuals in order to carry out its business and organisational functions.

1.2 Data Protection legislation defines 'personal data' as any information relating to an identified, or an identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, 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. Personal data also includes any expression of opinion about the data subject and what is intended for them.

1.3 The University is committed to protecting the rights and freedoms of individuals with respect to the processing of their personal data.

2. Purpose and Scope

2.1 The purpose this policy is to ensure compliance with the General Data Protection Regulation (GDPR) and related European Union (EU)[1] and national legislation ('Data Protection legislation'). Data Protection legislation applies to the processing of personal data about living identifiable individuals ('data subjects').

2.2 The University of Gloucestershire is registered with the Information Commissioner's Office (ICO) as a Data Controller. The policy incorporates guidance from the ICO, and outlines how the University will discharge its duties and obligations to comply with Data Protection legislation.

2.3 This policy applies to all parts of the University and to all personal data held and processed by the organisation. This includes data held in any system or format, whether electronic or manual.

2.5 This Policy applies to all members of staff except when acting in a private or non-University capacity. The term 'staff' means anyone working in any context within the University. This includes but is not limited to temporary, honorary, visiting, casual, voluntary and agency workers, students employed by the University, and external members of committees. This Policy also applies to all locations from which personal data is stored and accessed including off-campus.

2.7 This policy applies to all students when processing personal data on behalf of the University, but not in any other situation including when acting in a private or non-University capacity.

2.8 This policy also covers any staff and students who may be involved in research or other activity that requires them to process or have access to personal data. If this occurs, it is the responsibility of the relevant School or Unit to ensure the data is processed in accordance with Data Protection legislation and that students and staff are advised about their responsibilities. In addition, students and staff undertaking research must adhere to the Research Ethics: A

[1] See: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Handbook of Principles and Procedures[2], which provides information on ethical approval of research, privacy and confidentiality.

2.9 This policy is not, and should not be confused with, a Privacy Notice (a statement which informs data subjects how their personal data is used by the University).[3]

2.10 This policy should be read in conjunction with responsibilities and obligations outlined in the following documents, which supplement this policy where applicable:

2.10.1 Staff employment contracts and comparable documents which impose confidentiality obligations in respect of information held by the University;

2.10.2 Any other contractual obligations or staff policies which impose confidentiality or data management obligations in respect of information held by the University;

2.10.3 The Records Management Policy[4] and Records Retention Schedule[5] which govern the appropriate retention and disposal of University information;

2.10.4 The University's Data Breach Policy[6] which sets out the procedure to be followed if a personal data breach takes place;

2.10.5 IT and information security policies, procedures and terms and conditions which concern the confidentiality, integrity and availability of University information including rules about IT acceptable use[7], user accounts[8], internet[9], email[10], and network and wireless facilities[11].

3. Policy Statement

3.1 The University is committed to complying with Data Protection legislation through its everyday working practices.

3.2 Complying with Data Protection legislation may be summarised as, but is not limited to:

3.2.1 understanding, and applying as necessary, the data protection principles when processing personal data;

3.2.2 understanding, and fulfilling when necessary, the rights given to data subjects under Data Protection legislation;

3.2.3 understanding, and implementing as necessary, the University's accountability obligations[12] under Data Protection legislation.

---

[2] See: http://www.glos.ac.uk/docs/download/Research/handbook-of-principles-and-procedures.pdf
[3] Student / Staff Privacy Notices published here: http://www.glos.ac.uk/governance/information/Pages/data-protection.aspx
[4] See: http://www.glos.ac.uk/docs/download/Governance/records-management-policy-statement.pdf
[5] See: http://www.glos.ac.uk/docs/download/Governance/records-retention-schedule.pdf
[6] Data Breach Policy: http://www.glos.ac.uk/docs/download/Governance/data-breach-policy.pdf
[7] IT Acceptable Use Policy: http://www.glos.ac.uk/docs/download/Key/uap-18-04-18.pdf
[8] User Account Policy: http://www.glos.ac.uk/docs/download/Key/uap-18-04-18.pdf
[9] Internet Policy: http://www.glos.ac.uk/docs/download/Key/ip-18-04-18.pdf
[10] Email Policy: http://www.glos.ac.uk/docs/download/Key/ep-18-04-18.pdf
[11] Network and Wireless Policy: http://www.glos.ac.uk/docs/download/Key/nwp-18-04-18.pdf
[12] The accountability obligations include: implementing appropriate data protection policies; implementing data protection by design and default in projects, procurement and systems; using appropriate contracts with third party Data Controllers and Data Processors; holding relevant records about personal data processing; implementing appropriate technical and organisational security measures to protect personal data; reporting certain personal data breaches to the ICO; conducting Data Protection Impact Assessments where required; and ensuring adequate levels of protection when transferring personal data out of the European Economic Area.

3.3 In accordance with Data Protection legislation, additional conditions and safeguards will be applied to ensure that special category data (sensitive personal data) is handled appropriately. Special category personal data is information relating to an individual's:

3.3.1 race or ethnic origin;

3.3.2 political opinions;

3.3.3 religious beliefs or other beliefs of a similar nature;

3.3.4 trade union membership;

3.3.5 genetic data;

3.3.6 biometric data (where used for identification purposes);

3.3.7 health;

3.3.8 sex life or sexual orientation.

3.4 Criminal convictions or offences (alleged or proven) are not technically defined as special category personal data but are afforded similar protections.

4. Data Protection Principles

4.1 Data Protection legislation requires that the University, its staff and others who process or use any personal information, comply with the data protection principles.

4.2 The data protection principles state that personal data should be:

4.2.1 processed lawfully, fairly and in a transparent manner;

4.2.2 collected for specified, explicit and legitimate purposes;

4.2.3 adequate, relevant and limited to what is necessary;

4.2.4 accurate and where necessary kept up to date;

4.2.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data is processed;

4.2.6 processed in a manner that ensures appropriate security of the personal data.

4.3 Accountability is central to Data Protection legislation, and Data Controllers are responsible for compliance with the principles and must be able to demonstrate this to data subjects and the UK regulator, the ICO.

5. Data Subject Rights

5.1 The rights given to data subjects under Data Protection legislation are:

5.1.1 the right to be informed;

5.1.2 the right of access to the information held about them (though a Subject Access Request);

5.1.3 the right to rectification;

5.1.4 the right to erasure;

5.1.5 the right to restrict processing;

5.1.6 the right to data portability;

5.1.7 the right to object;

5.1.8 rights in relation to automated decision-making and profiling.

5.2 Under Data Protection Regulation legislation, data subjects have the right of access to their personal data held by the University.

5.3 Any individual who wishes to exercise this right should make the request through submitting a Subject Access Request Form[13] available on the University's website at: http://www.glos.ac.uk/governance/information/Pages/data-protection.aspx , or by contacting dataprotection@glos.ac.uk.

6. Roles and Responsibilities

6.1 As a Data Controller (or when acting as a joint Data Controller or a Data Processor), the University has a corporate responsibility for the following:

6.1.1 complying with Data Protection legislation and holding records to demonstrate this;

6.1.2 cooperating with the ICO, as the UK regulator of Data Protection legislation;

6.1.3 responding to regulatory / court action and paying administrative levies and fines issued by the ICO.

6.2 The University Executive Committee is responsible for reviewing and approving this policy.

6.3 University Council is responsible for assessing the overall risk profile of the University and ensuring appropriate resources and processes are in place and implemented to enable compliance with Data Protection legislation.

6.4 The University's Data Protection Officer is responsible for:

6.4.1 monitoring the University's compliance with Data Protection legislation including managing internal data protection activities, raising awareness, training, and the conduct of internal audit;

6.4.2 advising the University on its Data Protection obligations (including the use of Data Protection Impact Assessments);

6.4.3 acting as the University's point of contact for the ICO with regard to Data Protection legislation;

6.4.4 acting as an available point of contact for data subjects.

6.5 Governance and Secretariat Services[14], in collaboration with other relevant service areas, is responsible for:

6.5.1 providing advice, guidance, training and tools / methods to assist the University and staff in complying with this policy, in liaison with the Data Protection Officer, and taking account of ICO and other regulatory guidance and relevant case law;

6.5.2 publishing and maintaining core Privacy Notices and other University-wide data protection documents;

6.5.3 handling Subject Access Requests;

[13] Subject Access Request Form: http://www.glos.ac.uk/governance/information/pages/data-protection.aspx
[14] Within the Registrar's Directorate

6.5.4 advising on, managing and / or handling Data Protection Impact Assessments, data subject complaints, and personal data breaches, as advised by the Data Protection Officer.

6.6 Directors, Heads of School, and Heads of Professional Departments are responsible for:

6.6.1 ensuring that all staff within their areas are aware of this policy, and understand the role of data protection principles in their day-to-day working practices through induction, training, and performance monitoring;

6.6.2 ensuring that personal data within their areas is processed in line with this policy and associated policies and procedures;

6.6.3 supporting internal and external audits to ensure compliance with Data Protection legislation;

6.6.4 developing and reviewing information surveys to document information assets containing personal data in their areas, including databases, relevant filing systems, and the purposes of processing, to inform the University's Information Asset Register.

6.7 Compliance with Data Protection legislation is the personal responsibility of all members of the University who process personal data.

6.8 New members of staff are required to complete mandatory information governance online training as part of their University induction.

6.9 Staff members, as appropriate for their role and in order to enable the University to comply with Data Protection legislation, are responsible for:

6.9.1 completing the information governance online training, and refresher training annually and / or if their role changes significantly;

6.9.2 ensuring that any personal data they process adheres to this policy and any associated information security policies;

6.9.3 ensuring any personal data they process complies with the data protection principles;

6.9.4 following relevant advice, guidance and tools / methods provided in relation to information governance[15];

6.9.5 when processing personal data on behalf of the University, only using it as necessary for their contractual duties and / or other University roles and not disclosing it unnecessarily or inappropriately;

6.9.6 recognising, reporting internally with immediate effect, and cooperating with any remedial work arising from personal data breaches in accordance with the Data Breach Policy;

6.9.7 recognising, reporting internally with immediate effect, and cooperating with the fulfilment of Subject Access Requests;

6.9.8 when engaging with students who are using personal data in their studies and research, advising those students of relevant advice, guidance and tools / methods to enable them to handle such personal data in accordance with this policy;

6.9.9 ensuring they do not disclose personal data to a third party without establishing prior consent of the individual has been provided. This also includes information that would confirm whether or not an individual is or has been an applicant, student or employee of the University. The University may have a duty to disclose personal data to authorised

[15] Information Governance: https://infonet.glos.ac.uk/departments/registry/GSS/Pages/Infogov.aspx

bodies, such as the police and other organisations in order to comply with its legal or statutory obligations under Data Protection legislation. Any requests to disclose personal data for reasons relating to national security, crime and taxation should be directed to dataprotection@glos.ac.uk, who will respond on behalf of the University.

6.10 The responsibilities outlined under paragraph 6.9 apply to individual students when processing personal data on behalf of the University.

6.11 Any breach of this policy may be treated as misconduct under the University's relevant disciplinary procedures and could lead to disciplinary actions or sanctions.

7. Policy Review

7.1 This policy will be updated as necessary to reflect best practice, relevant case law, and to ensure compliance with any changes or amendments to Data Protection legislation.

7.2 This policy was last reviewed in May 2018. The policy was approved by the University Executive Committee in May 2018.