University of Westminster Personal Data Protection Policy

For Compliance with the General Data Protection Regulation & UK Law

1. Background

1.1 The General Data Protection Regulation (GDPR), enforceable from May 2018, has replaced the Data Protection Act 1998 as UK personal data protection law. This legislation is also supplemented by the Data Protection Act 2018.

1.2 This University personal data protection policy addresses the incorporation into all activities of the University the key principles and requirements of this new regulation.

1.3 The University of Westminster holds and uses personal data across a range of physical sites, functional departments, teaching colleges, schools and departments, in its information systems and in a variety of formats.

1.4 Personal information is vital to the operations and interests of the University and should be managed in all its forms with care and in compliance with the requirements of the GDPR and UK law.

1.5 This policy should be read in conjunction with specific published procedures and guidelines, available to the public, students and staff, as required.

1.6 The GDPR defines personal data as;

'Any information relating to an identified or 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 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.[1]

[1] The full regulation and all related definitions can be read at:

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

2. Scope

2.1 This policy covers all the activities and processes of the University that uses personal information in whatever format.

2.2 This policy relates to all University staff, students and others acting for or on behalf of the University or who are given access to University personal information.

3. Registration

3.1 In compliance with UK law, the University will register its processing of personal information with the Information Commissioner's Office. The current registration is **Z8450604**.

4. GDPR Principles, Articles and Recitals

4.1 The University of Westminster will manage the processing of personal information in compliance with the key GDPR principles and its relevant Articles and Recitals, as set out in the full Regulation, with the Data protection Act (2018) and with any relevant supporting guidance issued by the UK Information Commissioner.

The six key principles, in Article 5 of the GDPR, can be briefly summarised as:
Personal data shall be:
a) – processed lawfully, fairly and in a transparent manner in relation to the data subject ('**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, where allowed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes personal information will be collected for clear and specific purposes, shall not be considered 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 ('**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'**);

The University will adhere to these core principles.

In addition to these core principles, this policy commits the University to compliance with the Articles of the GDPR, its supporting Recitals and any official guidance on personal data protection available from the Information Commissioner's Office (ICO).

The GDPR and Recitals are available here:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

The ICO Guidance is available here:
https://ico.org.uk/for-organisations/guide-to-data-protection/

For the purposes of this policy, all University staff, agents and contractors are especially directed **to Appendix 1**, which provides references for key GDPR Articles and available ICO guidance.

Appendix 1 includes the GDPR text defining 'sensitive personal information' categories, now known as 'special category' personal data in the GDPR.

5. Personal Data Protection in Practice

The University of Westminster will comply with the GDPR, the Data Protection Act (2018) and other relevant UK law, specifically the University will undertake the following approaches:

5.1 Personal information collection and use

5.1.1 When personal information is collected, individuals will be told clearly what the information will be used for and who will have access to it, and if it is to be shared, who with and for what purpose. Article 13 will be followed in full.

5.1.2 Collection and use of personal information will be kept to a minimum to meet required purposes. Where it is possible to use anonymous information collection to fulfil required purposes, in research or general service feedback for example, these approaches should be encouraged.

5.1.3 Where personal information is being collected with the intention of using it for direct marketing purposes, individuals will be given the opportunity at the point of collection to refuse consent to direct marketing, in compliance with Privacy and Electronic Communications Regulations (PECR).

5.1.4 The University will apply approaches to personal information capture, use and maintenance that helps ensure personal information quality and reduces risks of inaccuracy and unnecessary duplication.
5.1.5 The University will create and maintain a Records Management Policy and related Records Retention Schedules to guide required personal information retention and timely destruction.

For further details, please see the University's Records Management Policy and Records Retention Schedules.

5.3 Personal Information Rights

The rights of information subjects, detailed in the GDPR Articles 15-21, will be respected and supported.

These include:
Right of Subject Access Right of Rectification
Right of Erasure (‘right to be forgotten’) Right to Restriction of Processing Right of Data Portability
Right to Object to Processing

The rights will be facilitated by a formal and published procedures, qualified where appropriate by specific reference to Articles and exemptions in the GDPR or UK law.

5.4 Business Change

The University will consider personal data protection in the context of required business changes and any associated IT changes and initiatives. Compliance to the GDPR and UK law will be considered fully in relation to business and IT options and changes and will be supported by appropriate project management frameworks and activities, including requirements for data protection impact assessments, as given in Article 35.

5.5 The Protection and Security of Personal Information

5.5.1 The University will create and maintain an Information Security Policy and an associated framework of technical measures and support, guidance and training to ensure appropriate levels of security are in place to adequately protect personal information it controls or processes, with reference to principle f) above and Article 32.

5.5.2 Security breaches will be monitored and subject to appropriate processes, activities and reporting with reference to Article 33. The GDPR requires breach reporting to be made to the ICO in a timely manner, within 72 hours if required. Staff should report all personal data breaches as soon as they are discovered.

5.5.3 Security policies and processes will encompass access to user accounts and the interception of communications for legitimate University purposes (for example to intercept email containing potentially damaging attachments or viruses) or where required to do so by law.

For further details, please see the University’s Information Security Policy.

5.6 Awareness and Training

The University will provide accessible guidance, support and training on the management of personal information and relevant legislation to all staff, students and those acting for or on behalf of the University. Staff will successfully pass awareness of security and information compliance before they undertake activities or are given access to systems that involve the processing of personal information.

6. Reviews and Continuous Improvement

6.1 Processes for managing personal information, including those that relate to corporate applications such as the Student Records System and HR system, will be periodically reviewed and any recommendations implemented as part of a continuous process of improvement.

6.2 The management of personal information in research will be subject to review, and where appropriate approval of a University research ethics committee or external approval by an equivalent body given.

6.3 Compliance to data subject rights requests and other formal requests for personal information will be monitored on a monthly basis and appropriate metrics recorded and reported to the line manager of Information Security and Compliance teams.

6.4 And further reported to the University Information Management Business Governance (Information Governance) Committee (IMBG-IG).

6.5 The University will supply metrics, information and views to external bodies, for example JISC or Committees of Parliament, to support the understanding and impact that personal data protection compliance has on the HEI and wider information management sectors, when requested, and if necessary resources are available.

7. Personal Information Management Policy Roles and Responsibilities

7.1 The University Personal Data Protection Policy is agreed by the IMBG-IG and formally approved by the University Information Management Committee. The University Library and Archives Service department, reporting to the Director of Student and Academic Services, is responsible for maintaining University Records Management Policy, Records Retention Schedules and all associated policies and training.

7.2 The Data Security Team, reporting to the Head of ICT Developments, Information Systems and Support, are responsible for the University Information Security Policy.

7.3 The Information Compliance Team, reporting to the Director of Strategy, Planning and Performance, are responsible for:

7.3.1 Maintaining this policy

7.3.2 Managing and reporting on formal subject rights requests and other formal requests for personal information.

7.3.3 Providing guidance, awareness, support and training on the management of Asset Registers, all personal information and relevant legislation.

7.3.4 Liaison with the Information Commissioner's Office on data protection

matters, including the reporting of data breaches.

7.3.5 Supplying metrics, information and views to external bodies in relation to personal data protection as thought appropriate.

8. Wider Personal Information Management Roles and Responsibilities

8.1 Heads of Professional Services, Colleges, Schools and other Heads of Business Units are responsible for ensuring general awareness and compliance with this policy in their areas. Specific training and support will be available from the Information Compliance Team.

8.2 Heads of Professional Services, Colleges, Schools and other Heads of Business Units will be considered University Information Asset Owners (IAO's) and will ensure, with the support of the Information Compliance Team, that Information Asset Registers and all other records of processing activities, as required by GDPR Article 30, are wholly adequate and kept up-to date, and can be made available to the Information Compliance Team or the Information Commissioner's Office on request.

8.3 IAO's will regularly report to the University's Senior Information Risk Officer (SIRO) on the status and risks associated with their Information Asset Register. The SIRO will report to the University's Vice Chancellor and President.

8.4 IAO's will be supported by designated Information Champions, or staff in an equivalent role in their functional area, who will monitor information flows, update documentation and Asset Registers, be involved in any required Data Privacy Impact Assessments and any other relevant data management and documentation activities.

8.5 All staff, students, contractors and agents who handle personal information, for or on behalf of the University, are responsible for its safety, security and compliance to the provisions of the GDPR and Data Protection Act 2018.

8.6 Any security breach or data damage or loss that affects personal information should be reported to the Data Security Team and Information Compliance Team, as agreed in the University Information Security Policy and related procedures. Security breaches or data damage or loss, including any loss of equipment that may hold University information, should be reported as soon as any breach, etc. is discovered.

8.7 Failure to report a suspected data security breach etc. and the mishandling of personal information in any instance could lead to a disciplinary investigation and additionally could be a breach of the law. Staff are advised to seek assistance and guidance from the Data Security Team or the Information Compliance Team if they have specific concerns in this area.

8.8 Data subject rights and information requests are granted in law and all staff involved in such requests should ensure requested information is made available to the Information Compliance Team in a timely and accurate manner. It should be noted that it is an offence to conceal, alter or destroy personal information to prevent it from being processed or reviewed that been the subject of a data rights

request.
Authorised by: University Information Governance Group Date:

Version Record

Version	Date	Author	Description
0.1	August 2017	M. Bacon - Information Compliance Manager	Draft – update of 2014 version to encompass GDPR and UK law.
1.0	10/01/18		Approved IMBG (IG) Version 0.1
1.5	29/3/2019	M. Bacon Information Compliance Manager	Draft following Internal Audit
2.0	01/05/2019	M. Bacon Information compliance Manager	Approved IMBG (IG) Version 2.0

Appendix 1 – Key GDPR Articles and ICO Guidance

For the GDPR and its Recitals see:
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

For ICO guidance related specifically to the GDPR see:
https://ico.org.uk/for-organisations/data-protection-reform/

The following is a brief GDPR Articles list that may be of special interest to this policy and the

Article 4 – Definitions
Key definitions of the GDPR including: personal data; processing; profiling; 'pseudonymisation'; controller; processor; consent; personal data breach; genetic data; biometric data; cross border processing; information society service; and other terms.

Article 5 – Principles relating to data processing
As given in the policy above.

Article 6 – Lawfulness of processing
The six possible legal basis for lawful processing.

Article 7 – Conditions for Consent
The conditions of evidence that need to be recorded for consent, clear presentation of the matter needing consent, rights of withdrawal and issues of consent in relation to the performance of a contract.

Article 8 – Child consent and information society services
Child consent and offers of information society services, i.e. access to web services, apps, etc.

Article 9 – Processing of special categories of personal data
Under the Data Protection Act these were known as 'sensitive personal data'. The GDPR now says:

1. Processing of personal data revealing **racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a**

natural person's sex life or sexual orientation shall be prohibited.

And then relates the specific conditions that allow processing of these kinds of special category personal data, the most important for many purposes being explicit consent.

Article 13 – Information to be provided where personal data are collected from the data subject

The specific information to be given to a data subject when their personal information is collected:
Identity of the data controller – most usually the University of Westminster.
Contact details for personal data protection issues – dpa@westminster.ac.uk
Purpose of the processing
Recipients of the data
Details of any transfers of data to a third country or international organisation and the related adequacy decision or safeguards in place and how to obtain a copy of these details
Retention period
Information rights
How to withdraw consent if that is the basis of processing
Right to lodge a complaint
Legal basis of processing
Any automated decision making, including profiling

Articles - 15 to 21 – Data Subject Rights

The rights of the data subject including:

Right of access
Right to rectification
Right to erasure ('right to be forgotten')
Right to restriction of processing
Right to data portability
Right to object

Article 22 – Automated individual decision making, including profiling

Right not to be subject to automated decision making processing unless based on explicit consent or limited circumstances.

Article 24 – Responsibility of the controller

The specific reference to implementing, "appropriate technical and organisational measures to ensure and **to be able to demonstrate** that processing is performed in accordance with this Regulation…" And the importance of appropriate data protection policies and adherence to approved codes of conduct.

Article 25 – Data protection by design and default
The article that introduces the concept of privacy by design, at the time of determination and implementation, and by default, by use of such things as data minimisation and 'pseudonymisation' to ensure the requirements of the GDPR are met.

Article 26 – Joint Controllers
Where two or more controllers jointly determine the purposes of processing, what they need to do is referenced here.

Article 28 - Processor
A key Article for consideration of those who offer or undertake the processing of personal information on behalf of the University. Processors must be able to meet all the requirements of the GDPR.

Article 30 – Records of Processing Activities
Processing activities need to be recorded, and need to contain the following details:

Data Controller, Joint Controller, DPO and all contact details
Purposes of processing
Categories of data subjects and categories of personal data
Recipient categories
Transfers to a third country or international organisation and suitable safeguards
Time limits for erasure of the different categories of data
Details of technical and organisational security measures

Records of processing carried out on the behalf of the controller need to be kept by processors and their representatives.

Records need to be made available to the supervisory authority, in the UK the Information Commissioner's Office, on request.

Article 32 – Security of Processing – Full Article

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) The pseudonymisation and encryption of personal data
(b) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services

(c) The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
(d) A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Article 33 – Notification of a personal data breach to the supervisory authority
When a data breach is likely to result in a risk to the rights and freedoms of natural persons, it must be reported no later than 72 hours after the organisation has become aware of it.

Article 34 – Communication of a personal data breach to the data subject
As above, in some cases the Data Controller must communicate data breaches to those affected.

Article 35 – Data Protection Impact Assessment
Prior to actual processing, in some cases, Data Controllers must carry out data protection impact assessments.

Article 36 – Prior Consultation
Where a data protection impact assessment has revealed a high risk to personal data processing with an absence of measures to mitigate those risks, the Data Controller must consult with the supervisory authority, on our case the ICO.

Article 37 – Designation of a Data Protection Officer
Universities are likely to be considered a public authority under GDPR. As such, we will have to designate a GDPR Data Protection Officer.

Article 38 – Position of the Data Protection Officer
The designated data protection officer has to be involved properly, in a timely manner, in all issues which relate to the protection of personal data. The GDPR data protection officer should be provided resources to:

Carry out all tasks
Have access to personal data and processing operations
Maintain expert knowledge

The GDPR data protection officer cannot be instructed on how related tasks should be carried out, cannot be dismissed for carrying out those tasks, and should report to the highest management level.

GDPR data protection officers can fulfil other tasks, but any such tasks or duties must not result in a conflict of interests.

Article 39 – Tasks of the data protection officer
These are the key tasks of the GDPR Data Protection Officer:

Inform the University and its staff of their obligations under the GDPR and UK data protection law.

- Monitor compliance to the regulation and its reflection in policies and staff responsibilities

- Raise staff awareness and training related to data protection and GDPR

- Provide advice in relation to data protection impact assessments

- Co-operate with the ICO

- Act as a contact point for the ICO

- Take into account the nature, scope, context and purposes of the processing in the University and have due regard for the risks associated with those processes.

Articles 44 – 50 International Data Transfers
These articles cover the legal requirements for transfers of personal data to third countries or international organisations. The University will conform to these requirements.

Article 83 – General Conditions for imposing administrative fines
This article defines the maximum administrative fines available to the ICO and other supervisory authorities. For information they are given below:

For infringements of obligations to Articles 8 (Child Consent), 11 (Processing not requiring identification), 25-39 (See Above) 42-43 (Certification)

Fines up to 10,000,000 EUR or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

For infringements of obligations relating to:
The basic principles for processing, including conditions for consent, Articles 5 (Principles), 6 (Lawfulness), 7 (Conditions of Consent), and 9 (Special Categories of Data);

Data Subject's Rights in Articles 12 – 22.

Transfers of personal data to a recipient in a third country or an international organisation regarding Articles 44 – 49.