Personal Data Protection Policy

1. Background

1.1 The processing of personal data in the United Kingdom is regulated by law. The principal legislation is the Data Protection Act 2018 (DPA 2018), the UK General Data Protection Regulation (GDPR), the Privacy and Electronic Communications Regulations (2003) and the Freedom of Information Act (2000). These laws are collectively referred to in this Policy as data protection legislation.

1.2 This personal data protection policy addresses the incorporation into all our activities the key principles and requirements of data protection legislation.

1.3 We (the University) hold and use personal data across a range of physical sites, functional departments, Colleges and Schools, in our information systems and in a variety of formats.

1.4 We process the personal data of a range of people including colleagues[1], students, representatives of partner organisations, contractors, researchers, suppliers and members of the public.

1.5 Personal information is vital to our operations and interests and should be managed in all its forms with care and in compliance with the requirements of data protection legislation.

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

1.7 The legislation 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[2].

1.8 Data protection legislation defines some types of personal data as likely to be more sensitive and gives them extra protection. This personal data is defined as special category personal data and includes:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;

[1] All references to colleagues in the policy means the employees of the University of Westminster.

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

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation)

- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

2. Scope

2.1 This policy covers all our activities and processes that use personal information in whatever format.

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

3. Scope

3.1. In compliance with UK law, we will register our processing of personal information with the Information Commissioner's Office (ICO).

4. GDPR Principles, Articles and Recitals

4.1. We will manage the processing of personal information in compliance with the UK 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.

In line with the key principles of the GDPR (highlighted below in bold), we will:

a) process personal data lawfully, fairly and in a transparent manner in relation to the data subject (**lawfulness, fairness and transparency'**);

b) collect personal data for specified, explicit and legitimate purposes and will not further process such data 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, shall not be considered incompatible with the initial purposes (**'purpose limitation'**);

c) ensure personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (**data minimisation'**);

d) ensure personal data is accurate and, where necessary, kept up to date; we will take every reasonable step to ensure that personal data that is inaccurate is erased or rectified without delay, having regard to the purposes for which it is processed, (**accuracy'**);

e) ensure personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed (**'storage limitation'**);

f) ensure personal data is 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'**).

4.2 As the controller, we shall be responsible for, and be able to demonstrate compliance with, a-f (**'accountability'**).

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

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

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

5 Personal Data Protection in Practice

5.1 Personal information collection and use

5.1.1 When we collect personal information, we will tell individuals 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. We will support this by the publication of privacy notices.

5.1.2 We will identify and record a lawful basis for processing for all processing of personal data.

5.1.3 We will keep collection and use of personal information 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, we will encourage these approaches.

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

5.1.5 We will apply approaches to data capture, use and maintenance that help ensure personal information quality and reduce risks of inaccuracy and unnecessary duplication.

5.1.6 We will create and maintain a Records Management Policy and related Records Retention Schedules[3] to guide required personal information retention and timely destruction. We will dispose of personal data in a secure manner. Further guidance can be found here.

5.2 Personal Information Rights

5.2.1 We recognise the legal rights of those whose data we process **and will ensure that appropriate information is provided to them advising them of their rights, and that policies and procedures are maintained to ensure that** we are **able to recognise information rights requests and handle them appropriately when they are exercised.**

5.2.2 These rights include the:

- Right to information about data processing operations
- Right of access to personal data (subject access requests)
- Right to portability of personal data
- Right of rectification of personal data
- Right of erasure of personal data (also known as the right to be forgotten)
- Right to restriction of processing

[3] For further details, please see the University's Records Management Policy and Records Retention Schedules [add link here].

- Right to object to direct marketing
- Right to object to data processing operations under some circumstances
- Right not to be subject to decisions made by automated processing under some circumstances
- Right of complaint about the organisation's processing of personal data

5.3 Business Change

5.3.1 We will consider personal data protection in the context of required business changes and any associated IT changes and initiatives. We will consider compliance with the requirements of data protection legislation fully in relation to business and IT options and changes, which we will support through appropriate project management frameworks and activities, including the requirement to conduct a Data Protection Impact Assessment (DPIA), as given in Article 35.

5.4 Protection and Security of Personal Information

5.4.1 We will create and maintain an Information Security Policy[4] and an associated framework of technical measures and support, guidance and training to ensure appropriate levels of security are in place to adequately protect the personal information we process. The level of security will be proportionate to the sensitivity of the processing as required by Article 32.

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

5.5 Data breaches

5.5.1 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

5.5.2 We will maintain a data breach reporting procedure. We will log, investigate and risk assess all data breaches. We will take appropriate remedial action as soon as possible to isolate and contain the breach, evaluate and minimise its impact, and to recover from the effects of the breach (including identifying actions to prevent such a breach re-occurring).

5.5.3 The GDPR requires data breaches where the rights and freedoms of individuals are likely to be affected to be reported to the ICO within 72 hours of the organisation becoming aware of the data breach. We will advise colleagues to report all personal data breaches as soon as they are discovered [5].

5.5.4 The GDPR requires that where a data breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms that individuals affected are notified. We will notify individuals affected without undue delay.

5.6 Awareness and Training

5.6.1 We will provide accessible guidance, support and training on the management of personal information and relevant legislation to all colleagues, and to those acting for or on behalf of the University. All new colleagues will undertake information security and data protection training when they join the University.

[4] For further details, please see the University's Information Security Policy [add link here].
[5] Details of how to report can be found on the Information Compliance intranet pages [add link here].

6 Reviews and Continuous Improvement

6.1 We will review periodically processes for managing personal information, including those that relate to corporate applications such as the Student Records System and HR system. We will implement any recommendations from the review as part of a continuous process of improvement.

6.2 We will review the management of personal information in research, and where appropriate will require approval from the University Research and Knowledge Exchange Ethics Committee or an equivalent external body.

6.3 We will monitor compliance in responding to data subject rights requests and other formal requests for personal information quarterly, recording appropriate metrics. The Information Governance Advisory Group (IGAG) will review the metrics [at each meeting/periodically/quarterly/annually?].

6.4 When requested, and if necessary resources are available, we 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 higher education and wider information management sectors.

7 Policy Roles and Responsibilities

7.1 This Policy is subject to the approval of the University Secretary and Chief Operating Officer on the recommendation of IGAG.

7.2 The Library and Archives Service, reporting to the Associate Director of Digital Engagement and Library Services in Student and Academic Services is responsible for maintaining the Records Management Policy, Records Retention Schedules and all associated policies and training.

7.3 The Data Security Team, reporting to the Head of IT Developments in Information Systems and Support, are responsible for the Information Security Policy.

7.4 The Information Compliance Team (managed by the Information Compliance Manager/Data Protection Officer) and reporting to the Head of University Governance, are responsible for:

7.4.1 Maintaining this policy

7.4.2 Managing the response to personal data breaches and identifying remedial actions (with relevant colleagues)

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

7.4.4 Providing guidance, awareness, support and training on the management of all personal information and advising on relevant legislation.

7.4.5 Liaison with the ICO on data protection matters, including the reporting of data breaches.

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

7.4.7 Keeping and maintaining records of personal data processing.

8 Wider Roles and Responsibilities

8.1 Directors of Professional Services and other directorates, Heads of Colleges, Heads of 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 on request from the Information Compliance Team.

8.2 Directors of Professional Services and other directorates, Heads of Colleges, Heads of Schools and other Heads of Business Units are Information Asset Owners (IAOs) 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.

8.3 The Data Protection Officer will regularly report to the Senior Information Risk Officer (SIRO) on the status of any high-risk processing of personal data. The SIRO will report, as appropriate, to the University Executive Board.

8.4 The Information Compliance Team will support IAOs to update documentation and review Information Asset Registers, will be involved in any required DPIAs and any other relevant data management and documentation activities.

8.5 IAOs will ensure that any data protection breaches are swiftly brought to the attention of the Information Compliance team and that they support the Information Compliance team in investigating and resolving breaches.

8.6 IAOs will ensure that personal data held electronically is protected using secure passwords and/or access controls is kept and destroyed securely. Additionally, they will ensure paper files and other records or documents containing personal and/or special category data are kept securely and destroyed securely.

8.7 We reserve the right to contract out data processing activities or operations involving the processing of personal data to third parties, in the interests of business efficiency and effectiveness. We will not appoint any third-party data processor who is unable to provide satisfactory assurances that they will handle personal data in accordance with data protection legislation.

8.8 All colleagues, students, contractors and agents who handle personal information, for or on behalf of the University, are responsible for its safety, security and compliance with the provisions of data protection legislation.

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

8.10 Data subject rights and information requests are granted in law and all colleagues involved in such requests should ensure requested information is made available to the Information Compliance Team in a timely and accurate manner. Note: it is an offence to conceal, alter or destroy personal information that has been requested via a Subject Access Request to prevent it from being processed, reviewed or disclosed.

9 Failure to adhere to the requirements of this policy

9.1 Failure to report a suspected data breach and/or the mishandling of personal information in any instance could lead to a disciplinary investigation.

10 Policy review

10.1 The Information Compliance Manager will review this policy annually in collaboration with relevant stakeholders and IGAG.

10.2 The policy is subject to the approval of the University Secretary and Chief Operating Officer on the recommendation of IGAG.

11 Digital accessibility

11.1 We are committed to ensuring our websites and content is digitally accessible according to the Public Sector Bodies Accessibility Regulations (2018). This policy is published on our website; and can be requested in a range of formats e.g. Word, PDF, plain text, alternative formats such as large print or Braille.

12 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
2.5	12/12/2022	M. Bacon Information Compliance Manager	Updated
2.5	12/01/2023	M. Bacon Information Compliance Manager	Approved IGAG Review January 2026
3.0	25/03/2025	N Cooke Information Compliance Manager	Approved by IGAG (Feb 25) Approved by USCOO and UEB (Mar 25) Review January 2026

Appendix 1 – Key GDPR Articles and ICO Guidance

For the GDPR and its Recitals see:

https://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:

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

Definition of special category data

There are specific conditions that allow the processing of these kinds of 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

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 ICO, 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 they are 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 DPO 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 DPO 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 DPOs 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 with 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. We 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.