UNIVERSITY OF
LEADING
THE WAY
WESTMINSTER

Data Protection Impact Assessment (DPIA) 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)[1], 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 policy should be read in conjunction with the Personal Data Protection Policy.

1.3 Under the above legislation we (the University) as a Data Controller have an obligation to incorporate necessary safeguards into all activities that involve the processing of personal data; this is known as 'data protection by design'.

1.4 A key element in data protection by design is the requirement to undertake a Data Protection Impact Assessment (DPIA), sometimes also referred to as a 'Privacy Impact Assessment' (PIA), where any processing of personal data is "likely to result in a high risk" to the rights and freedoms of individuals. See Appendix One DPIA Screening Questions below and the Information Commisioner's Office (ICO) Guidance.

1.5 A DPIA serves as a tool to help us identify, evaluate and mitigate risks to identifiable individuals arising out of the processing of their personal data.

1.6 Failure to undertake a DPIA when required by law could result in sanctions or fines from the governing authority, which in the UK is the ICO.

2. Scope

2.1 This policy applies to all Colleges, Schools, Professional Services and other directorates and other business units and covers all our activities.

3. Roles and Responsibilities

3.1 All colleagues involved in the development of projects, initiatives, studies, surveys, processes, and systems (known from this point as an 'initiative') are responsible for ensuring that they are aware of this policy and understand the circumstances in which a DPIA should be undertaken.

3.2 Our Data Protection Officer is responsible for overseeing and reviewing the implementation of this Policy and must be consulted in relation to any DPIAs undertaken in accordance with the policy's requirements. The DPO will consult the Information Governance Advisory Group (IGAG) where a DPIA indicates highly sensitive processing of personal data.

3.3 In practice, it is the responsibility of the colleague or team leading an initiative to undertake the screening questions and produce a first draft of a DPIA, i.e., the Business Relationship Manager, Business Analyst, Project Manager, System Owner, Principal Investigator etc. The Data Protection Officer and the Information Compliance Team and other relevant stakeholders, including third party suppliers, can then assist with further elaboration and completion.

[1] See GDPR.

3.4 You should send information about DPIAs and early draft DPIAs to the Information Compliance Team at dpa@westminster.ac.uk.

3.5 You should send DPIAs that are initiated as part of IT procurement, IT development or with an IT element to Information Systems and Support (ISS) Developments – Data Security by raising a Service Desk request or by email to cybersecurity@westminster.ac.uk.

4. Identifying the need for a DPIA

4.1 You must undertake a DPIA **before** the processing of any personal data which is likely to result in a high risk to the rights and freedoms of individuals. You must therefore identify whether there are any factors that require the need for a DPIA to be undertaken.

4.2 The GDPR requires a DPIA to be undertaken where any initiative will involve:

4.2.1 The systematic and extensive evaluation of personal data by automated means, including profiling, resulting in decisions that would have significant effects for those individuals.

4.2.2 The processing of special categories of personal data or personal data relating to criminal convictions and offences on a large scale; or

4.2.3 The systematic monitoring of a publicly accessible area on a large scale.

4.3 Where any new initiative will involve the processing of personal data, you should complete the DPIA screening questions in Appendix One. These questions should be completed by those leading and knowing most about the intentions of the Initiative.

4.4 Before completing the questionnaire, it is important that you identify key stakeholders in the initiative so they can provide their input to the questions and have a clear understanding of the scope and objectives of the initiative so the questionnaire can be completed as accurately as possible.

4.5 If in any doubt about the applicability of any of the screening questions, consult with the Information Compliance Team and the Data Protection Officer, as necessary.

4.6 Where the outcome of the DPIA questionnaire suggests that the initiative is unlikely to result in a high risk to individuals, there may be circumstances where it is advisable to undertake a DPIA anyway due to;

4.6.1 The nature, scope, context and purposes of processing personal data.

4.6.2 The individuals affected by the processing (e.g., vulnerable adults, children, etc).

4.6.3 The strategic nature or level of investment in the initiative in terms of time, finances, and other resources.

4.6.4 The importance and visibility of the initiative internally and externally.

4.7 If you conclude that a DPIA is not necessary and will not be undertaken in relation to any initiative, you should retain the questionnaire and document any supporting reasons to evidence the decision you made. You should submit these to the Information Compliance Team at dpa@westminster.ac.uk as they may need to be revisited and reviewed later.

5. Undertaking a DPIA

5.1 If having completed the questionnaire you establish that a DPIA is necessary or desirable for a specific initiative, you should complete the full DPIA template in Appendix One.

5.2 The sections of the DPIA form allow you to describe the initiative in both diagram and text and to capture the key privacy risks, risk controls and control owners and that eventual implementation is agreed and signed off.

5.3 Completing the DPIA runs alongside other initiative tasks, but you should complete the DPIA **prior** to starting any processing of the personal data it describes.

5.4 It is likely you will need to involve relevant internal and external stakeholders to complete the DPIA successfully. If this involves any third-party data processors (service providers), the contract they have with the University should cover an obligation to assist us in undertaking DPIAs as necessary. However, this may have cost implications which you may need to discuss and agree with third parties beforehand.

5.5 We must identify the lawful basis for all processing of personal information. The GDPR identifies the following list. Which basis is most appropriate to use will depend on the purpose for processing and the relationship with the individual.

a) **Consent**: the individual has given clear consent for the processing of their personal data for a specific purpose. Consent must be freely given and can be withdrawn at any time.

b) **Contract**: the processing is necessary for a contract with the individual, or because they have asked that we take specific steps before entering into a contract.

c) **Legal obligation**: the processing is necessary for us to comply with the law (not including contractual obligations).

d) **Vital interests**: the processing is necessary to protect someone's life. This normally applies to the processing that the emergency services carry out and is unlikely to apply to processing we carry out.

e) **Public task**: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

f) **Legitimate interests**: the processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. Please note this condition cannot apply to the statutory functions of a public body.

5.6 In addition, special category data can only be processed if one of the specific conditions in Article 9 of the UK GDPR are met. Which is most relevant will depend on the nature of the processing.

5.7 Article 9 conditions are:

a) Explicit consent
b) Employment, social security and social protection (if authorised by law)
c) Vital interests
d) Not-for-profit bodies
e) Made public by the data subject
f) Legal claims or judicial acts
g) Reasons of substantial public interest (with a basis in law)
h) Health or social care (with a basis in law)
i) Public health (with a basis in law)
j) Archiving, research and statistics (with a basis in law)

5.8 For further guidance please refer to the Processing of Special Category and Criminal Convictions Data Policy and/or refer to the Information Compliance Team.

6. Review of DPIAs

6.1 You should undertake a DPIA at the earliest opportunity in the development of an initiative. The DPIA should be subject to ongoing assessment and review prior to any eventual completion and an initiative going live. This is to ensure the initiative is accurately reflected in the DPIA and the controls and measures it covers are adequate for the risks identified and all these controls have been integrated into the initiative.

6.2 For initiatives that are part of IT procurement, IT development or with an IT element, your DPIA should follow a process agreed with the ISS Business Relationship Managers and the Digital Transformation

Team. See Appendix Two for details.

6.3 In normal circumstances we expect that the identification of privacy risks and their controls and mediation will reduce the overall privacy risk related to any initiative to low or at most medium. Our Risk Appetite in this area is low to medium; the Head of Cyber Security or a cyber security representative and the Data Protection Officer may approve DPIAs of this level of risk without further authorisation.

6.4 The Senior Information Risk Officer (SIRO) and key stakeholders will consider any initiative's DPIA if privacy risks remain high after the suggested controls and mediation. Any introduction of these risks into normal University business will be exceptional and will be subject to consultation with the ICO.

6.5 Once you commence the processing in any DPIA, you should log the authorised DPIA as completed and make it available to the key stakeholders. Any future changes to processing within the scope of an existing DPIA could trigger another DPIA and an updated set of documentation.

6.6 DPIAs should include Records of Processing information at the time of the Initiative implementation. Completion of the DPIA should prompt the updating of the relevant information asset records and privacy notices.

7. Consultation with the Information Commissioner's Office

7.1 If the outcome of a DPIA is that the processing of personal data in the context of the initiative would result in a high risk and it is not possible to take any measures to eliminate or mitigate that risk, and the SIRO and stakeholders wish to proceed with the Initiative, the GDPR requires that we consults with the ICO **before any processing relating to the Initiative takes place.**

7.2 The Data Protection Officer will initiate contact with the ICO, which is likely to happen only in very exceptional circumstances and on the instruction of the SIRO.

7.3 The Data Protection Officer will send a copy of the DPIA and a covering note with all relevant information to the ICO.

7.4 Further activity on the initiative will only take place in consultation with the ICO, which may cover providing additional information. In some cases, the ICO will confirm that the risks and mitigations described are acceptable to them or in others they may recommend that the processing is not undertaken.

8. Disclosure and publication of DPIAs

8.1 You should keep a record of the DPIA with any project or initiative that requires one. The Information Compliance Team will maintain a log of completed DPIAs. The DPIA will be considered complete when it is signed off by either the Data Protection Officer or the SIRO.

8.2 There is no legal requirement to disclose or publish DPIAs, although we are a public authority subject to the Freedom of Information Act 2000 (FOIA). Information held about DPIAs may be disclosed in response to questions raised under the FOIA if we cannot apply an applicable exemption.

8.3 We will redact any published, disclosed or shared DPIA to remove any personal, confidential or commercially sensitive information as applicable.

9. Policy Review

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

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

10. Related policies

10.1 This policy forms part of our information security management system (ISMS) and should be read in conjunction with our other information management policies, which are reviewed and updated as necessary to maintain an effective ISMS to meet our business needs and legal obligations.

11. Digital accessibility

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

11.2 This policy is published on our website at https://www.westminster.ac.uk/about-us/our-university/corporate-information/policies-and-documents-a-z.

12. Version record

Version	Date	Author	Description
0.5	December 2021	M. Bacon - Information Compliance Manager	Draft for comment and approval – update of 2018 DPIA form and process.
1.0	April 2022	M. Bacon and includes IGAG comments.	Version 1.0
1.0	April 2022	Approved by IGAG	Version 1.0
1.5	March 2025	N Cooke – Information Compliance Manager	Updates agreed by IGAG (Feb 25) Approved by USCOO and UEB (Mar 25) Review January 2026

Appendix One – DPIA Questionnaire and Template Form

Data Protection Impact Assessment (DPIA)

(for help and guidance in completing this form please contact the Information compliance team at DPA@westminster.ac.uk)

DPIA authors	
Service / School	
Title	
ISS reference (where applicable)	
Date completed	

Screening question – are you….. *Please answer yes/no to each questions. If you're answer is 'yes' to any of the below, please complete the form. If 'no' please submit your completed form to DPA@westminster.ac.uk*	**Yes/No**
Evaluating or scoring individuals (including profiling and predicting)?	
Conducting automated decision-making?	
Systematically monitoring individuals or groups?	
Processing any sensitive personal data?	
Processing personal data on a large scale?	
Matching or combining datasets containing personal data?	
Processing personal data of vulnerable people?	
Using new or changed technology solutions (including use of a new third party suppliers)?	
Using innovative technology solutions (including any use of artificial intelligence)?	
Transferring personal data outside of the European Union (including use of cloud solutions)?	
Restricting an individual(s) from exercising their rights under data protection legislation?	

Context Provide a description and the context of the personal data processing. What are the intended outcomes? Why and how is the personal data processed? By which organisation(s)? Whose personal information will be processed e.g. students, alumni, third parties? What volume of information will be processed and how often? Will you be processing children's data?

Types of personal data *Please state what personal data you will be processing.*			
Personal data	**Yes/No**	**Special category personal data**	**Yes/No**
Name		Race	
Address		Ethnic origin	
Email address		Political opinions	
Telephone numbers		Religious or philosophical beliefs	
Date of birth		Trade union membership	
Gender		Genetic data	
Financial information e.g. card number, salary, income		Biometric data	
Education and qualifications		Health data	
Location data (including mobile phone tracking and IP addresses)		Sex life	
Residency data/eligibility to live in the UK		Sexual orientation	
Images or recorded footage		Crime data e.g. criminal convictions or allegations, witness statements	
Unique identifiers e.g. passport number, NHS number			
Other (please state)			

Lawful basis for processing personal data *To process personal data organisations need to identify a lawful basis. Further guidance can be found here for personal data and here for special category personal data.*			
Basis for processing personal data		**Basis for processing special category personal data**	
Consent: the individual has given clear consent for you to process their personal data for a specific purpose		**Consent:** the individual has given clear consent for you to process their personal data for a specific purpose	
Contract: the processing is necessary for a contract you have with the individual		**Made public by the data subject:** the individual has disclosed the data themselves	
Legal obligation: the processing is necessary for you to comply with the law Please state which legislation applies:		**Employment, social security and social protection law:** processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field	
Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law		**Legal claims and judicial acts:** necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity	
Vital interests: the processing is necessary to protect someone's life		**Vital interests:** the processing is necessary to protect someone's life	

Legitimate interests: the processing is necessary for your legitimate interests unless there is a good reason to protect the individual's personal data which overrides those interests. This cannot apply where a public authority is processing data to perform official tasks		**Health or social care:** necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems	
		Substantial public interest: necessary for reasons of substantial public interest, on the basis of Domestic Law which shall be proportionate to the aim pursued	
		Not-for-profit bodies: processing is carried out in the course of its legitimate activities with appropriate safeguards and relates solely to the members or to former members of the body	
		Public health: necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care	
		Archiving, research and statistics: for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes • necessary for that purpose – it is a reasonable and proportionate way of achieving your purpose, you must not have more data than you need; • subject to appropriate safeguards for people's rights and freedoms; • not likely to cause someone substantial damage or substantial distress; • not used for measures or decisions about particular people, except for approved medical research; and • in the public interest.	
		Processing criminal offence data: personal data relating to criminal convictions and offences or related security measures • necessary for that purpose – it is a reasonable and proportionate way of achieving your purpose, you must not have more data than you need; • subject to appropriate safeguards for people's rights and freedoms; • not likely to cause someone substantial damage or substantial distress; • not used for measures or decisions about particular people, except for approved medical research; and • in the public interest.	

Systems and Storage
What software will be used to manage the personal data? If this is software provided by a third party, please provide details? Has a contract been drawn up with the third party which includes data protection clauses? Where in the world is the data held? Will this system link with any others or export data? How will access to the system be controlled? What backup and recovery procedures will be put in place?

Technical diagram Use diagrams and text to map and describe the data flows

Retention What will the retention period be? How will data be disposed of when no longer needed? How will data be preserved (if required)?

Identification of privacy risks

Please use this table to document any risks you have identified

Risk ID	**Privacy risk** *e.g. No privacy policy or statement covering personal data collections.*	**Impact** *What impact in relation to a person would the risk have – High, Medium or Low*	**Likelihood** *What is the likelihood of this risk having that impact if left uncontrolled – High, Medium or Low*	**Mitigation** *What controls will be put in place to mitigate the risk?*	**Due date**	**Managed by** Insert name
01						
02						
03						
04						
05						

Consultation

Please state who has been consulted regarding this personal data processing?

Team/Role	**Name**
Project manager	

Data management and security	
Supplier representative	
University Business Representative	
University Business Relationship Manager	
Business Sponsor	
Information Compliance Team	

Data Protection Officer Assessment *When you have completed this form, please send it to DPA@westminster.ac.uk. The organisations Data Protection Officer will assess the privacy implications in accordance with the legislative requirements below. You may be asked to provide further information.*			
DPA principle	**Yes/No**	**Comment**	**Action required**
Processed lawfully, fairly and in a transparent manner			
Collected for specified, explicit and legitimate purposes			
Relevant and limited to only what is necessary			
Accurate and where necessary kept up to date			
Retained only for as long as necessary			
Processed in an appropriate manner to maintain security			

Signoff	
Name	
Date	

Appendix Two – ISS DPIA Process