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 Data Use and Access Act 2025 (DUAA), 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. Please click here for guidance from the Information Commission (IC) .

1.5 A DPIA serves as a tool to help us identify, evaluate and mitigate privacy 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 IC.

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 report to 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, completion and signoff.

[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 Additionally 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.

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

- Evaluation or scoring.
- Automated decision-making with legal or similar significant effect.
- Systematic monitoring.
- Sensitive data or data of a highly personal nature.
- Data processed on a large scale.
- Matching or combining datasets.
- Data concerning vulnerable data subjects.
- Innovative use or applying new technological or organisational solutions.
- Preventing data subjects from exercising a right or using a service or contract

4.3 Where any new initiative will involve the processing of personal data, you should complete the DPIA screening questions on the DPIA template. 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 by writing to DPA@westminster.ac.uk.

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;

- The nature, scope, context and purposes of processing personal data.
- The individuals affected by the processing (e.g., vulnerable adults, children, etc).
- The strategic nature or level of investment in the initiative in terms of time, finances, and other resources.
- 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 screening questions you establish that a DPIA is necessary or desirable for a specific initiative, you should complete the full DPIA template.

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 concerns, risk controls and control owners.

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. Data protection legislation 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.

g) **Recognised legitimate interest**: is a specified purpose for handling personal information that is in the public interest. These pre-approved purposes are the recognised legitimate interest conditions;

(a) Sharing personal data with another organisation that has requested it from you because they need it for their public task or official functions (the 'public task disclosure request condition');
(b) safeguard national security, protect public security or for defense reasons (the 'national security, public security and defense condition');
(c) respond to, or deal with, an emergency situation (the 'emergencies condition');
(d) prevent, detect or investigate crimes, including the apprehension and prosecution of offenders (the 'crime condition'); or
(e) protect the physical, mental or emotional well-being of people who need extra support to do this or protect them from harm or neglect (the 'safeguarding condition').
(f)

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, signoff 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 One 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 IC.

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 Completion of the DPIA should prompt the updating of the relevant information asset records and privacy notices.

7. Consultation with the Information Commission

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 UK GDPR requires that we consults with the IC **before any processing relating to the Initiative takes place.**

7.2 The Data Protection Officer will initiate contact with the IC, 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 IC.

7.4 Further activity on the initiative will only take place in consultation with the IC, which may cover providing additional information. In some cases, the IC 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 bi-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 (February 2025) Approved by USCOO and reported to UEB (March 2025) Review January 2026
1.6	March 2026	N Cooke – Information Compliance Manager	Updates agreed by IGAG (February 2026) Approved by USCOO and reported to UEB (March 2026) Review January 2028

Appendix One – ISS DPIA Process