Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

colegsirgâr

colegceredigion

Data Protection Impact Assessment (DPIA)

Data Protection Impact Assessment

The instrument for a privacy impact assessment (PIA) or data protection impact assessment (DPIA) was introduced with Article 35 of the General Data Protection Regulation (GDPR).

- Impact Assessment is a process to help you identify and minimise the data protection risks of a policy or a project.

- An impact assessment (DPIA) should be completed:

  (a) at the outset of any project that involves the collection or handling of personal information;
  (b) when any new policy is proposed that will require the collection or handling of personal information;
  (c) where there is a proposed change to an existing policy, system or process that involves the collection or handling of personal information.

- A good impact assessment helps to evidence consideration of the risks related to the intended processing, and that the University has considered all relevant data protection obligations.
- Impact assessment also helps to identify and remedy privacy and security issues at an early stage; fixing issues reactively further down the line can often be expensive or technically impossible.
- To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.[1]

Further information:

ICO Privacy Impact Assessment Code of Practice

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

The attached template should be used for undertaking a DPIA. It may be modified to meet the needs of the activity being assessed, provided that the key elements are covered. It follows the approach recommended by the UCISA Privacy Impact Assessment Toolkit and the Information Commissioner's Office Code of Practice.

Queries relating to the completion of a DPIA can be obtained from the University's Head of Data Protection : foi@uwtsd.ac.uk.

[1] Information Commissioner

1. This document records the outcome of a Data Protection Impact Assessment for

[insert details]

at the University of Wales Trinity Saint David, ICO registration number Z6441030.

2. Please provide a brief introduction to the initiative

[What is it? Who is it going to affect? When is it likely to happen? Does it replace or update something people are already familiar with?]

3. Step One – Identify the need for a PIA

(click in the box to indicate yes/no as appropriate)

1. Will the project involve the collection of new information about individuals?
   Yes □ No □

2. Will the project compel individuals to provide information about themselves?
   Yes □ No □

3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
   Yes □ No □

4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
   Yes □ No □

5. Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, inter alia, the use of biometrics or facial recognition?
   Yes □ No □

6. Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
   Yes □ No □

7. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.
   Yes □ No □

8. Will the project require you to contact individuals in ways which they may find intrusive?
   Yes □ No □

9. Will the project introduce new facilities that might be used by individuals in the institution to gather, process, analyse or share personal information in ways that would previously have required specialist support?
   Yes □ No □

10. Will the project involve the processing of personal data by third parties (third parties would include all cloud based services)?
    Yes □ No □

11. Will the project expose personal data to elevated levels of security risks?
    Yes □ No □

12. Are stakeholders likely to have privacy concerns about the project?
    Yes □ No □

⇨ **If your answers to the questions have all been No**, there is no requirement for a full assessment to be made.

If this is the case, please send a copy of the completed form to:
foi@uwtsd.ac.uk

Please make sure that the completed form is also submitted to the committee that will be authorising the document / policy. This will need to be considered as part of the decision-making process.

⇨ **If you have answered 'Yes' to any of the questions**, please continue and complete Step Two.

---

4. Step Two – Describe the information flows

Please provide a detailed description of the information to be processed, how it is processed and how it flows.

5. Step Three – Identify and assess risks

This section is to identify potential or actual risk in relation to the protection of personal data, based on the information you have provided in step two. Please outline below any identified risks associated and control measures that can reduce or eliminate the risk.

Use the information tables on Impact and Likelihood to help you with scores in columns (d), (e), (f) and (g).

		Pre-control				Post-control		
Ref:	Risk (descriptor)	Likelihood (d)	Impact (e)	Risk level (d)x(e)	Control measures	Likelihood (f)	Impact (g)	Risk level (f)x(g)
	For example, 'A' leads to 'B' resulting in 'C' (this should include a description of the impact on individuals, compliance or the reputation of the institution.	*1 - 5*	*1 - 5*			*1 - 5*	*1 - 5*	
1								
2								
3								
4								
5								

Impact

	Individuals	Compliance	Reputation
1	None	None	None
2	A data breach resulting in the sharing/loss/use of data that does not identity an individual.	Requires notification to Head of Data Protection for assessment of remedial steps.	Negligible, no impact on student recruitment, government perception or public opinion.
3	A data breach resulting in the sharing/loss/use of data that identities an individual, which is already publically available elsewhere.	Sharing of data without permission requires notification to Head of Data Protection for assessment of notification individuals concerned, to ICO and UWTSD internal investigation.	Will / may have short-term (weeks) impact on student recruitment, government perception or public opinion.
4	A data breach resulting in the sharing/loss/use of data that identities an individual, and leads to some material or non-material damage.	Will result in disclosure of the breach to the ICO. May result in penalty.	Will / may have medium-term (months) impact on student recruitment, government perception or public opinion.
5	A data breach resulting in the sharing/loss/use of data that identities an individual and impacts upon an individual's rights and freedoms.	Will result in disclosure of the breach to the ICO. May result in licence suspension / revocation.	Will / may have long-term (a year or longer) impact on student recruitment, government perception or public opinion.

Likelihood

Likelihood Score	Descriptor	Description
1	Highly Unlikely (0 -10%)	The event may occur only in the most exceptional of circumstances
2	Unlikely (11- 40%)	Not expected to occur
3	Likely (41 – 60%)	The event is expected to occur at some time
4	Very Likely (61- 90%)	The event will occur in most circumstances.
5	Certain (91- 100%)	Event is certain to occur

Step Four – Identify any additional actions

This section identifies whether any additional actions need to be taken to appropriately manage the risks identified in Step Three. In doing so, the University accepts that the control measures (identified in step three) and additional measures below are sufficient and appropriate to protect the data of individuals.

Risk ref	Additional Action required	By whom	By when

6. Step Five - Approval process

Upon completion, this form and any supporting documentation should be submitted to the Head of Data Protection who will check that the document complies with University requirements.

Policies: Policies should be formally considered and approved in accordance with Committee Terms of Reference outlined in the Academic Quality Handbook. Where data impact has been identified this completed Data Protection Impact Assessment must be submitted along with the relevant policy / document / in order for approval to be sought. If the policy affects staff, advice should be sought from HR at the outset to ascertain if consultation is required at JCC. HR will also provide advice on the most appropriate stage to consult with JCC and on whether approval by Council is required.

Impact Assessed Activities: This impact assessment forms a planning and compliance component of activity delivery. Where data impact has been identified, and impact assessment undertaken, it should be considered and approved by the project lead/heads with responsibility for delivery, to inform decision-making and mitigate risk.

7. For completion by the Head of Data Protection

I confirm that this Data Protection Impact Assessment has been completed appropriately ☐ **Date**:

Summary of any additional advice / matters requiring consideration by the approving committee/head of delivery: