PRIVACY IMPACT ASSESSMENT POLICY

Department	Strategic Planning		
Author	Legal Services Advisor		
Authorised By:	Associate Director of Strategic Planning		
Implementation By:	Associate Director of Strategic Planning		
Policy Reference:	POSP1718007		
Policy Replaced:	NA		
Version No:	1	**Approval Committee:**	VCB
Date approved:	17.04.18	**Minute no:**	17.96.05
Status:	Approved	**Implementation Date:**	May 18
Period of approval:	3 years	**Review Date:**	May 21

I have carried out an equality impact assessment screening to help safeguard against discrimination and promote equality.	✓
I have considered the impact of the Policy/Strategy/Procedure *(delete as appropriate)* on the Welsh language and Welsh language provision within the University.	✓

EXPLANATIONS OF TERMS USED

Accreditation of Information Assets – The small scale and full scale PIA will form part of the accreditation documentation for an Information Asset

Information Asset – An Information Asset is Service User, student, staff or corporate information / data, processed by us and is held in an electronic or hard copy/manual format. Therefore, we are the data controller.

GDPR – The General Data Protection Regulation

Personal Confidential Data – is data for example such as name, postcode, GP, next of kin, address, date of birth etc.

Privacy Impact Assessment – (PIA's) A risk technique advocated by the ICO to enable organisations to address privacy concerns and ensure appropriate safeguards are addressed and built in as projects or plans to develop existing information assets.

Projects / plans to develop – PIA's are required when new projects occur (for example introduction of a new electronic human resources or payroll) or where plans are proposed to develop an existing information asset. These can be both paper and electronic

Sensitive Data – under the Data Protection Act 1998 is data for example such as patient diagnosis, medical history, ethnicity, sex, religion.

PRIVACY IMPACT ASSESSMENT POLICY

Introduction

This Privacy Impact Assessment (‘PIA’) policy is applicable to any member of staff who are responsible for project managing a new “project” or “plan” to modify any existing system (information asset).

NEW projects that involve personal confidential data or intrusive technologies give rise to privacy issues and concerns. Privacy embraces “confidentiality” and “student consent” and as an overarching principle this policy advocates that respect for student and staff privacy and dignity should be considered at the outset of any project, which embraces confidentiality and student and staff consent. To enable the University to address the privacy concerns and risks, a technique referred to as Privacy Impact Assessment (PIA), as advocated by the Information Commissioner, **must** be used **See Appendix 1 ‘Privacy Impact Assessment’.**

As we are a public authority organisation we are registered under the Data Protection Act 1998 with the ICO as data controller under registration number Z5199192 *to ‘enable us to provide education and support services to our students and staff; advertising and promoting the university and the services we offer; publication of the university magazine and alumni relations, undertaking research and fundraising; managing our accounts and records and providing commercial activities to our clients. We also process personal information for the use of CCTV systems to monitor and collect visual images for the purposes of security and the prevention and detection of crime*’. Therefore, we process students and staff information which is classified as Personal Confidential Data (PCD) and sensitive data.

What is a data protection impact assessment?

Data protection impact assessments are the same as privacy impact assessments or PIAs) which are a tool which can help the University identify the most effective way to comply with our data protection obligations and meet individuals’ expectations of privacy. An effective DPIA will allow us to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

The ICO has promoted the use of DPIAs as an integral part of taking a privacy by design approach.

See the ICO’s conducting privacy impact assessments code of practice for good practice advice.

The University must comply with the GDPR, the Data Protection Act 1998 (as amended) and other UK Privacy Laws when we process such information. The University has drafted this policy following the ICO PIA good practice guidance and screening questions outlined in **Appendix 1.**

You must carry out a DPIA when using new technologies and the processing is likely to result in a high risk to the rights and freedoms of individuals. By way of example, this would include a change in the student admission programme or a new HR programme for staff or payroll/finance. This is because the programme is not the University’s but actually ‘owned’ by the developer of the programme or tool we would use. The ‘owner’ will have given the University rights or a licence to use their programme, therefore, they would have a way of having access to that data. The University needs to ascertain who has access and if a 3rd party has ability to see the data.

Processing that is likely to result in a high risk includes (but is not limited to):

- systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals.

- large scale processing of special categories of data or personal data relation to criminal convictions or offences.

  This includes processing a considerable amount of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to rights and freedoms e.g. based on the sensitivity of the processing activity.

- large scale, systematic monitoring of public areas (CCTV).

What information should the DPIA contain?

(i) A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller *(see Article 6 GDPR which sets out the lawful processing conditions akin to Schedule 2 Data Protection Act).*

(ii) An assessment of the necessity and proportionality of the processing in relation to the purpose.

(iii) An assessment of the risks to individuals.

(iv) The measures in place to address risk, including security and to demonstrate that you comply.

(v) A DPIA can address more than one project.

The relevant provisions in the GDPR – see Articles 35, 36 and 83 and Recitals 84, 89 and 96

What type of PIA should I complete?

For all information systems new or currently in place a small-scale PIA will be completed first. This will then be followed by a Full-scale PIA.

Small-scale PIA
Similar to a full-scale PIA, but is less formalised. Requires less exhaustive information gathering and analysis. More likely to be used when focusing on specific aspects of a project

Full-scale PIA
Conducts a more in-depth internal assessment of privacy risks and liabilities. Analyses privacy risks, consults widely with stakeholders on privacy concerns and brings forward solutions to accept, mitigate or avoid them.

Privacy Impact Assessment guidance is provided for staff members by the Data Protection Officer, as part of the Information Asset Owner training. The Data Protection Officer is also responsible for ensuring support and guidance is given when staff members are required to fill out the Privacy Impact Assessment.

PURPOSE

The aim of a Privacy Impact Assessment is to ensure that systems and processes within the University are fit for purpose and include privacy by design. The confidentiality and the protection of the information within the information asset **must** be assessed. There must also be a comprehensive consideration of potential impacts on information quality and security at the design phase of any new process or procurement of a new information asset.

Privacy by design

Benefits of taking a ‘privacy by design’ approach:

Taking a privacy by design approach is an essential tool in minimising privacy risks and building trust. Designing projects, processes, products or systems with privacy in mind at the outset can lead to benefits which include:

- Potential problems are identified at an early stage, when addressing them will often be simpler and less costly.
- Increased awareness of privacy and data protection across an organisation.
- Organisations are more likely to meet their legal obligations and less likely to breach the Data Protection Act.
- Actions are less likely to be privacy intrusive and have a negative impact on individuals.

SCOPE

The scope of this document is to outline the University’s approach and methodology for Privacy Impact Assessments for, current systems that have not had a PIA before and also **NEW** systems.

It covers all information assets that are paper or electronic within the University.

This Policy covers all staff employed by the University, private contractors, volunteers and temporary staff.

DUTIES AND RESPONSIBILITIES

The adherence to the PIA Policy and procedures is essential for assuring aspects of the Information Governance Committee terms of reference and agenda, this is maintained and supported by

Vice Chancellor

The University’s Accountable Officer is the Vice Chancellor who has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. Information risk is handled in a similar manner to other risks such as financial, legal and reputational risks.

Reference to the management of information risks and associated information governance practice is now required in the Statement of Internal Control which the Accounting Officer is required to sign annually.

SIRO (Senior Information Risk Owner)

The SIRO is the Director of Human Resources. The SIRO is a Vice Chancellor Executive Team (VCET) member with allocated lead responsibility for the University’s information risks and provides a focus for the management of information risk at Board level.

The SIRO key responsibilities are;

- ensure that this policy and the information security objectives are compatible with the strategic direction of the University;

- ensure that data and information assets are identified; that the top level data and information governance roles are allocated and that the post-holders are appropriately briefed on their information security roles and carry out their functions with due diligence;
- own the risks associated with the information security objectives and ensure that control action owners are identified;
- ensure that exception procedures are in place to authorise at an appropriate level acceptance or mitigation of significant information security risks that deviate from agreed standards;
- determine when and by whom breaches of information security shall be reported to relevant external authorities;
- ensure there is clear direction and visible management support for security initiatives and promote continual improvement;
- ensure the Vice-Chancellor, the University and the Board of Governors are adequately briefed on risk management issues.

Data Protection Officer

The Data Protection Officer is responsible for ensuring the organisation meets its statutory and corporate responsibilities and is also accountable for:

- ensuring effective management, accountability, compliance and assurance for all aspects of Information Governance;

- ensuring that in line with the IG Committee terms of reference appropriate measures are taken to ensure that adequate consideration is given to the Privacy Impact Assessment;

- providing support for staff members required to complete the PIA by providing Information Asset Owner Training and further support to complete the PIA as deemed necessary

Information Asset Owners (IAO) – Directors, Associate Directors, Heads of School, Managers Etc.

The SIRO is supported by departmental / section IAOs who are senior managers involved in running the relevant services. Their role is to understand what information is held, what is added, and what is removed, how information is moved, who has access and why. As a result, they are able to understand and address risks to information assets they “own” and to provide assurance to the SIRO on the security and use of the assets. All IAO’s employment contracts reflect their responsibilities for information governance

Information Asset Administrators (IAA)

IAA’s work with an information asset on a day to day basis. They have day to day responsibility, ensure that policies and procedures are followed by staff and recognise actual or potential security incidents, and consult their IAO on incidents. They may also be known as the Application Manager for an Information System.

Information Security

The Associate Director of Information Services is responsible for the provision and management of a high quality, customer focussed, Information Technology Security Service using expertise to manage security issues, identifying best practice and making recommendations for local implementation.

PIA MANANGEMENT PROCESS

The Information Asset Management Process and the PIA

Privacy Impact Assessments need to be completed at an early stage of the project **BEFORE** the new ‘proposed’ system is procured or **BEFORE** the planned ‘change’ has taken place as part of the Information Asset Management Process.

The next section illustrates the important stages and/or information for consideration when looking at procuring new systems or changing those already used by the University. The aim is to ensure that all elements of a project that may impact upon the ability of the University to protect its data are being considered.

PIA PROCESS

The appointed Information Asset Owner is responsible for ensuring the PIA is completed and that the PIA is carried out with support and guidance from other individuals as relevant, i.e. The Data Protection Officer, Associate Director for IS.

The following process **must** be followed:

STEP 1

a. Inform appropriate Leads (Directors / Associate Directors/Heads of School) on the process for New System / Process or Proposed change to an Information System. Communication is essential to ensure compliance with checklist and processes.

STEP 2

a. Data Protection Officer will start the Accreditation of Information Asset documentation by forwarding this policy to the Information Asset Owner.

b. Initial Information Governance Security Checklist to be carried out by the Information Asset Owner / Information Asset Administrator. (*SMALL SCALE PIA*)

c. PIA will be carried out, supported by the Data Protection Officer. If an electronic system is involved, advice and support from the Associate Director for ICT Services.

d. Once identified that the system holds Person Confidential Data and Sensitive Data, full scale PIA to be completed, with the support of the Data Protection Officer.

e. Where non-compliance is identified in the small / full scale PIA then risk assessments completed, risks highlighted to SIRO where required

STEP 3

a. A Procurement Process starts; informed by results of IT and IG checks and PIA.

b. An action plan for ensuring PIAs are embedded in the life cycle of the Information Asset.

c. Data Protection Officer will progress Accreditation Information Asset document in line with the development of the project.

d. Data Protection Officer will ensure that all Accreditation of Information Asset documents are approved by the SIRO in conjunction with the Deputy Siro and the University Legal Adviser and a process of audit and review is put in place.

In following this process and ensuring that Data Protection Officer are notified and involved from the initial conception of the project we can provide assurance the University's information is being handled in a secure and responsible way and complies with UK Law.

Note: The PIA is only applicable where the proposed new project/system/process or proposed change to a system/process is to use personal confidential data (PCD) along with sensitive data, or significantly change the way in which personal data is handled

As a result of a completed Privacy Impact Assessment an action plan must be devised and written up for initial approval and subsequent auditing and monitoring by the IG steering group.

This ensures that information risks are recorded, mitigation put in place with an annual review to ensure on-going compliance with confidentiality, data protection and security.

Please follow the procedure laid down in Appendix A of this document to complete the PIA.

TRAINING

Guidance on the nature of the Privacy Impact Assessments will be provided to Information Asset Owners and Administrators. This will involve bespoke training by the Data Protection Officer called "Information Asset Owner Training".

All Information Asset Owners (IAOs) will be made aware of their responsibilities for the protection of their Information Assets through generic and specific training programmes and guidance.

IAOs need to have an understanding of:

- what a privacy impact assessment is and what information assets to apply it to;
- what information assets they are responsible for;
- when to apply a PIA;
- how it links into the procurement or implementation of a new system;
- how to incorporate the action plans into a project plan;
- knowing who to contact to get advice and guidance.

EQUALITY IMPACT ASSESSMENT

All relevant persons are required to comply with this document and must demonstrate sensitivity and competence in relation to the nine protected characteristics as defined by the Equality Act 2010. If you, or any other groups, believe you are disadvantaged by anything contained in this document please contact the Equality and Diversity Officer in HR who will then actively respond to the enquiry.

PROCESS FOR MONITORING COMPLIANCE

Overall monitoring will be the responsibility of the SIRO and Deputy SIRO, however, the Data Protection Officer role will be to provide regular reports and monitoring to the SIRO.

Monitoring will be through:

- Action Plans from PIA;
- Risk Assessment Action Plans;
- Project Risk and Issues logs;
- Audit of PIA process on an annual basis;

- Audit of PIA documentation.

Shortfalls identified will be discussed at the Information Governance Committee and Action Plan(s) devised.

CROSS REFERENCE TO OTHER PROCEDURAL DOCUMENTS

Data Protection Policy
Freedom of Information Policy
Information Security Policy
Risk Management Policy and Procedures

All current policies and procedures are accessible in the policy section of the public website (on the home page, click on ‘Policies and Procedures’). University Guidance is accessible to staff on the University Intranet.

APPENDIX A

PROCEDURE FOR PIA

The aim of a Privacy Impact Assessment is to ensure that systems and processes within the University are fit for purpose. Some of the considerations that must be taken into account are whether a new (or modified) project /process or information asset will:

- Ensure the necessary consents have been obtained from those whose personal data is being used;
- Affect the quality of personal information already collected;
- Allow personal information to be checked for relevancy, accuracy and validity;
- Incorporate a procedure to ensure that personal information is disposed of through archiving or destruction when it is no longer required in line with the University's retention and destruction guidelines;
- Have an adequate level of security to ensure that personal information is protected from unlawful or unauthorised access and from accidental loss, destruction, breaches of confidentiality or damage;
- Enable data retrieval to support business continuity in the event of emergencies or disasters;
- Enable the timely location and retrieval of personal information to meet subject access requests;
- Alter the way in which the organisation records in or monitors and reports information from a key organisational system.

Please see the screening questions which are intended to help you decide whether a PIA is necessary.

Please complete as much as you can and seek the Data Protection Officer advice when you run in to problems