**University of Wales**

**Trinity Saint David**

**Data Breach Policy**

Contents

[1. Introduction 3](#_Toc160012830)

[2. Deﬁnitions 3](#_Toc160012831)

[3. Purpose of this policy 3](#_Toc160012832)

[4. Reporting a personal data breach 4](#_Toc160012833)

[5. Breach management 4](#_Toc160012834)

[6. Personal data breaches resulting from cyber security incidents 6](#_Toc160012835)

[7. Evaluation and ‘lessons learnt’ 6](#_Toc160012836)

# Introduction

* 1. University of Wales Trinity Saint David Group and University of Wales (“the University”) collects, processes and retains data in order to deliver its operational and strategic objectives and to support its business functions.
	2. When processing personal data, the University has a legal obligation to ensure that it complies with the requirements made in the United Kingdom General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and any other related legislation, including the EU GDPR if applicable.
	3. As part of those legal obligations, the University must ensure appropriate safeguards exist to protect personal data.
	4. If these safeguards fail, the University has a legal duty to maintain processes for the detection, reporting and management of incidents involving the breach of personal data.

# Deﬁnitions

* 1. For the purposes of this policy, ‘personal data’ is deﬁned as information relating to natural persons who:
		+ can be identiﬁed or who are identiﬁable, directly from the information in question or
		+ can be indirectly identiﬁed from that information in combination with other information.
	2. This policy applies to personal data for which the University is the registered data controller and is also applicable when an external party is processing such data.
	3. ‘Data breach’ is deﬁned as an incident where there has been a breach of security around personal data which has in turn lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

# Purpose of this policy

* 1. This policy details how the University meets its legal obligations around the reporting and management of personal data breaches, by:
		+ detailing the procedure by which staff must report personal data breaches to the designated Data Protection Ofﬁcer (DPO); and
		+ conﬁrming the duty of staff to assist the DPO and their staff in respect to the handling of personal data breaches; and
		+ outlining the factors which must be considered when risk assessing the impact and severity of a personal data breach; and
		+ establishing the institutional framework within which data breaches must be managed and recorded, in order to reduce the impact, severity and risk associated with data breaches.

# Reporting a personal data breach

* 1. On becoming aware of a potential breach of personal data, staff must immediately report the breach to the DPO.
	2. When reporting a breach, staff are required to provide the following information to the DPO:
		+ a description of the personal data affected;
		+ an explanation of the incident, how it happened and when;
		+ the types and approximate number of data subjects concerned;
		+ the categories and approximate number of personal data records concerned;
		+ the likely consequences of the personal data breach;
		+ any immediate attempts to reduce the impact of the breach.
	3. Staff will be asked to complete the Data Incident Evaluation Report Form (“DIERF”) attached at Appendix A. Lack of clarity around the circumstances surrounding the potential breach must not delay the reporting of breaches to the DPO.
	4. Staff must assist the DPO in a timely manner to any queries raised by the DPO during any the investigation and/or associated investigations.
	5. The University may appoint external processors to process data on its behalf. Any associated contract must require the processor to inform without delay the University’s DPO of any potential personal data breach affecting University controlled data.
	6. If a staff member at the University becomes aware that a processor or sub-processor has experienced a personal data breach, they must inform the DPO as they would any other breach.
	7. The DPO must take reasonable steps to ensure that all staff are aware of the reporting mechanism contained in this section.

# Breach management

* 1. On receipt of the DIERF the DPO will assess whether the potential breach is likely to result in a material risk to the rights and freedoms of the data subjects concerned.
	2. If the DPO considers the potential breach would result in a likely material risk to the rights and freedoms of the data subject, they shall report the breach to the University Secretary as soon as is practicable and then to the Information Commissioner’s Ofﬁce (ICO) within 72 hours of UWTSD becoming aware of the breach. The University Secretary will subsequently report the breach and the ICO’s response to HEFCW and the Audit and Risk Committee using the established protocol for reporting, and will liaise with the Chairs of the Audit and Risk Committee and the Council to determine whether a report should be made to the Charity Commission.
	3. Where a breach or potential breach is not deemed to be reportable, the DPO shall deﬁne the breach or potential breach as a ‘data security incident’ or ‘non-reportable data breach’ and report the matter to the University Secretary. The breach will be logged in the University’s “breach log”.
	4. When assessing the risk posed by the breach to data subjects, the DPO shall consider the following factors:
		+ the type of breach;
		+ the nature, sensitivity and volume of personal data;
		+ ease of identiﬁcation of individuals;
		+ severity of consequences to individuals;
		+ special characteristics of the individuals affected;
		+ the number of affected individuals.
	5. Where there is a lack of detail around the causes and potential impact of a breach, the DPO should include that as a factor when assessing the overall risk.
	6. Where there has been a serious breach deemed to be reportable to the ICO (and the DPO has identiﬁed a high risk to data subjects) the DPO will contact the data subjects concerned, without undue delay and informing them of, as a minimum:
		+ a description of the nature of the breach;
		+ the name and contact details of the DPO and/or other relevant contacts;
		+ a description of the likely consequences of the breach;
		+ a description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.
	7. All breaches will be investigated by the DPO
	8. The DPO will advise and assist the reporting department to take steps to contain any potential breach, mitigate any resulting risks and put in place remedies so as to reduce the impact of any potential breaches on the data subject(s) concerned.
	9. If, during the course of the investigation, the DPO uncovers further information that changes the nature of a minor data breach so that it appears that the breach is reportable, the DPO will consult with the University Secretary to confirm the action to be taken.
	10. The DPO/the University will assist the ICO in the exercise of its statutory powers concerning reportable data breaches and will consider any advice given by the ICO around the management of a reported data breach.
	11. The DPO will maintain a log of all breaches (the breach log), reportable as well as minor, as well as a record of all actions and decisions made by the Data Protection Ofﬁcer in respect of the management of that breach.

# Personal data breaches resulting from cyber security incidents

* 1. In circumstances where the security of personal data has been compromised by a cyber-incident, rather than a specific data breach, the DPO will liaise with senior colleagues in the University’s Digital Services area, in accordance with the IT Incident Response Plan, ensuring that the cyber incident is managed according to the requirements made in this policy and other policies. The University Secretary will be kept informed at all times.

# Evaluation and ‘lessons learnt’

* 1. Once the personal data breach has been contained and remedial actions completed, the DPO shall review the causes of the personal data beach and the University’s response to the breach.
	2. The DPO’s evaluation will be communicated to the University’s senior management of the operational area in which the breach occurred.
	3. The evaluation will also be communicated to the University Secretary to ensure a ‘lessons learnt’ approach is embedded in the data breach process.
	4. The DPO will include relevant statistics and summaries around data breaches in their regular reports to the University Secretary for reporting processes.

**Appendix 1**

 **Data Incident Report Evaluation Form**

1. **Date and time of Incident (and when it came to your attention)**
2. **Describe the incident that took place (what happened, how it happened, what steps you took to mitigate the loss, for example recalling an email sent in error)**
3. **Provide detail of the data and the number of people who may be affected by the incident/data breach**

**Name…………………………………………………………………………………**

**Date and Time……………………………………………………………….**

**Please ensure the information provided is as full as possible and contact the University’s Data Protection Officer as quickly as possible to report the breach.**

Policy author(s):

Paul Osborne – Data Protection Officer

Document version control

|  |  |  |  |
| --- | --- | --- | --- |
| Version No: | Reason for change: | Author: | Date of change: |
| 0.1 | Policy created | PO | 1st Feb 2024 |
| 0.2 | Policy reviewed by Deputy University Secretary and added to corporate template | RD and CG | 28th Feb 2024 |
|  | Approval by SLT |  | 8th November 2024 |
|  |  |  |  |

Current status of Policy: agreed by SLT

Is the Policy applicable to**:** / Both FE and HE\*

Date ratified: 8/11/24

Date effective from: 8/11/24

Policy review date: 7/11/25

For publication**:** on / MyDay /

### *Approval*

*The policy will be formally considered and approved in accordance with Committee Terms of Reference outlined in the Academic Quality Handbook.*

*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*

*ALL policies submitted for approval must be accompanied by a completed:*

* [*Equality and Welsh Language Impact Assessment*](https://uowtsd.sharepoint.com/%3Aw%3A/r/corporate-services/Shared%20Documents/Policies%20%26%20Strategies/Guidance%20and%20Templates/1.3%20UWTSD%20Equality%20and%20welsh%20language%20Impact%20Assessment%20March%202022%20v2.dot?d=w108478d73dff429290b3881e7312c242&csf=1&web=1&e=ieoDH6)
* [*Institutional Impact Assessment*](https://uowtsd.sharepoint.com/%3Aw%3A/r/corporate-services/Shared%20Documents/Policies%20%26%20Strategies/Guidance%20and%20Templates/1.4.%20UWTSD%20Institutional%20Impact%20Assessment%20-%20Oct%202017.dotx?d=wa000b736a38941ff992940a724f79bce&csf=1&web=1&e=dMgUao)
* [*Data Protection Impact Assessment*](https://uowtsd.sharepoint.com/%3Aw%3A/r/corporate-services/Shared%20Documents/Policies%20%26%20Strategies/Guidance%20and%20Templates/Data%20Protection%20Impact%20Assessment%20template.dotx?d=w806d26e953bc46f5bc6c3243f4bed39a&csf=1&web=1&e=hyeTgg)

*Prior to submission to committee, authors are asked to consult the Policy and Planning Team who will check that the document complies with University requirements. The Policy and Planning Team will complete the section below.*

***For completion by the committee secretary***

*Please tick to confirm the following:*

*An institutional Impact Assessment has been completed* [x]

*An EIA and Welsh Language Assessment has been completed* [x]

*A DPIA has been completed* [x]

*Matters requiring consideration by the approving committee:*

