

## 10. APPENDIX 1

### DATA PROTECTION INCIDENT REPORTING FORM

The aim of this form is to ensure that in the event of a security incident such as data loss, all information can be gathered to understand the impact of the incident and what must be done to reduce any risk to students and others data and information. **Please act promptly to report any data incidents.** If you discover a personal data security incident, please notify your Line Manager, Dean, Head of Department or Director immediately.

Please complete Section 1 of this form and return it to the Data Protection Officer at [dpo@glyndwr.ac.uk](mailto:dpo@glyndwr.ac.uk) as soon as possible.

<b>Section 1: Notification of Data Security Incident</b>	<b>To be completed by person reporting incident/person who triggered incident or their Line Manager</b>
<b>Date incident was discovered:</b>	
<b>Date of Incident:</b> <i>Date and time of incident. When, what, who, how was it discovered. Full description of how the incident occurred.</i>	
<b>Place of incident:</b>	
<b>Name of person reporting incident:</b>	
<b>Contact details of person reporting the incident</b> ( <i>email address and telephone number</i> )	
<b>Brief description of incident or details of the information lost:</b>	
<b>Number of data subjects affected if known:</b>	
<b>Has any personal data been placed at risk?</b> <i>If so, please provide details</i>	
<b>Brief description of any action taken at the time of discovery:</b>	
<b>For use by the Data Protection Officer</b>	
<b>Received by:</b>	
<b>On (date):</b>	

This form is also available in [Welsh](#).

<b>Forwarded for action to:</b>	
<b>On (date):</b>	
<b>Any Additional Comments</b>	
<b>Section 2: Assessment of Severity</b>	To be completed by the Lead Investigation Officer in consultation with the Dean or Director affected by the incident plus DPO and if appropriate, IS.
<b>Details of the IT systems, equipment, devices, records involved in the IT security breach:</b>	
<b>Details of information loss:</b>	
<b>How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT system?</b>	
<b>How many data subjects affected?</b>	
<b>Is the data bound by any contractual security arrangements? E.g. Commercial contracts/data processing agreements.</b>	
<b>What is the nature of the sensitivity of the data? Please see the classification scale and insert the classification. If deemed High Risk, please also complete the following:</b>	
<b>Can any of the information be used to commit identity fraud such as: personal bank account and other financial information; national identifiers, such as National insurance number and copies of passports and visas?</b>	
<b>Detailed profiles of individuals including information about work performance, salaries or personal life that could cause significant damage or distress to that person if disclosed?</b>	
<b>Spreadsheets of marks or grades obtained by students, information about individual cases of student</b>	

This form is also available in [Welsh](#).

discipline or sensitive negotiations which could adversely affect individuals?	
Security information that would compromise the safety of individuals if disclosed?	

<b>Lead Investigation Officer to give to DPO</b>	
Date:	
Forwarded to action to:	
Assessment: Breach/Incident/Near Miss	
Incident Log Number:	
Any Additional Comments:	
<b>Section 3: Action Taken</b>	<b>To be completed by DPO</b>
Report Received by:	
On (date):	
Has this been reported to ICO? <i>If yes, within 72 hours?</i>	
Which officers have been interviewed?	
Details of when the employee completed Data Protection Training:	
Was incident reported to the Police? <i>If yes, notified on date?</i>	
Has there been any media coverage of the incident? <i>If so, please provide details:</i>	
Will a SIGI Panel be convened? <i>If so, date of Panel:</i>	
If no SIGI Panel is to be convened, please outline the justifications for <b>not</b> doing so:	
Follow up action required/recommended:	
Any Procedural changes in place to prevent this type of loss occurring again?	
<b>FOR USE BY THE SIRO/DPO:</b>	
Notification to ICO:	<b>YES/NO</b> <i>If YES, notified on:</i>
	<b>Details:</b>

This form is also available in [Welsh](#).

<b>Notification to Data Subjects:</b>	<b>YES/NO</b> <i>If YES, notified on:</i>  <b>Details:</b>
<b>Notification to other external regulator/stakeholder</b> <i>e.g. Charities Commission/HEFCW</i>	<b>YES/NO</b> <i>If YES, notified on:</i>  <b>Details:</b>

This form is also available in [Welsh](#).

*This form is also available in [Welsh](#).*

*This form is also available in [Welsh](#).*