MANAGEMENT CONTROL HEADER			
Department	Legal		
Author	University Solicitor		
Authorised By:	Information Governance Committee		
Implementation By:	SIRO/Data Protection Officer		
Procedure Reference:	PRLEG2122003		
Procedure Replaced:	PRSP1718008		
Version No:	2	**Approval Committee:**	VCB
Date approved:	03.05.22	**Minute no:**	21.97.06.02
Status:	Approved	**Implementation Date:**	May 2022
Period of approval:	3 years	**Review Date:**	May 2025
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 on the Welsh language and Welsh language provision within the University.			☐✓

SERIOUS INFORMATION GOVERNANCE INCIDENT PROCEDURE

1. Introduction and Overview

1.1 What is a Serious Information Governance Incident (SIGI)?

1.1.1 A Serious Information Governance Incident or a personal data breach occurs when there is:

A breach of security leading to the accidental or unlawful destruction, loss alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

This incident could also affect an individual's privacy, lead to identity fraud or have some other significant impact on individuals.

1.1.2 A Serious Information Governance Incident is likely to constitute a breach of the **Data Protection Act 2018** as amended.

1.2 What causes a SIGI?

1.2.1 The Information Commissioner's Office

States that a SIGI / data security breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack (social engineering, phishing etc)
- 'Blagging' offences where information is obtained by deceiving the organisation that holds it

1.2.2 Other reasons for a breach occurring could include:

- Poor disposal of confidential waste
- Unauthorised disclosure of confidential information to a third party (in any format including verbal)
- Finding confidential information / records in a public area
- Sharing of computer IDs and passwords

1.3 How can a SIGI be managed?

1.3.1 When an incident occurs, there are four important elements to the incident management plan:

- Containment and recovery
- Assessment of on-going risk
- Notification
- Evaluation and response (these categories are separate in this document).

1.3.2 It is important that staff recognise when an incident has occurred and report it appropriately so that immediate action can be taken to contain it. Failure to report a serious information governance incident within 24 hours of discovery could result in a disciplinary offence.

1.3.3 The University has a duty to report any significant breach to the ICO within 72 hours. Failure to report a significant breach to the ICO within 72 hours of discovery could result in a fine, intervention and damage to the University's reputation.

1.3.4 All serious information governance incidents should be reported in the first instance to your Line Manager using the form in Appendix 1, Section 1 and then reported to and logged with the Data Protection Officer and the SIRO, Executive

Director of Human Resources, who will provide advice on the next steps and any immediate action required to contain the incident. They may also recommend that your line manager liaises with Human Resources to determine whether or not any immediate action concerning employees needs to be taken.

1.3.5 Please Note that there are two further Deputy SIROs at the University in the absence of the University SIRO or DPO, they can be contacted on dpo@glyndwr.ac.uk

The next section of this procedure outlines what should be done to manage a data protection breach.

2. How to Manage an Incident – In Detail

2.1 Containment and Recovery

2.1.1 The person discovering an information governance incident/data protection breach should report it immediately as follows:

- to their Line Manager or Dean/Director
- to the SIRO via p.gibbs@glyndwr.ac.uk or dpo@glyndwr.ac.uk or telephone 01978 293995 who will:
    - log the incident
    - advise on the next steps and any immediate action required to contain the incident
- take advice from HR directly or advise that the line manager takes advice from HR regarding any immediate action which may need to be taken regarding employees
- contact IS if any IS equipment is involved in the incident

At this point the SIRO will decide who will be the appropriate investigating officer (usually the line manager, Director or Dean) who will start a full investigation without delay, following which he or she will complete the form at Appendix 1 Section 2. The completed form will be sent to the DPO who will complete Section 3 of the form in Appendix 1 and send to the SIRO/Deputy SIRO.

2.1.2 The investigating officer should ensure they obtain all the pertinent facts regarding the incident, take possession of any documentation and record any key facts/decisions from this point forward.

2.1.3 As a minimum, this should include;

- Date and time of the incident
- Who was involved
- Exactly what information has been disclosed (attach a copy to the form if it

has been recovered)

- How the breach occurred
- Whether the data has been recovered
- Whether the data subjects involved have been informed
- What immediate corrective action has been taken
- Further actions planned, who is responsible for ensuring they are carried out and when they will be completed

2.1.4 Depending on the type and seriousness of the incident, the police may need to be involved at any of these early stages and the member/s of staff suspended from the work place. This decision will be taken by the SIRO on a case-by-case basis.

2.1.5 Once the investigating officer is fully appraised of the incident by the SIRO, they may also need to contact officers as per below depending on the type of incident, if these officers are not already involved in the investigation. **All incidents are to be treated as urgent to minimise any further risks involved;** therefore, key staff must be contacted within 24 hours of the incident being discovered: If IT security is involved, report to ITS helpdesk or to Director of IS, Private & Confidential – itservicedesk@glyndwr.ac.uk or telephone 01978 293241

2.1.6 If the incident involves personal information of employees, the SIRO should, if appropriate, inform the Head of Human Resources (Operations & Systems) via danielle.sullivan@glyndwr.ac.uk or by contacting 01978 293921

2.1.7 If the incident has involved a disclosure of personal information which may leave the data subject at risk for some reason e.g. financial information or information which indicates they are vulnerable in some way, immediate notification should be considered to minimise this risk (see section 4).

2.1.8 If required, resources should be made available to facilitate the investigation process.

2.2 Setting up a containment exercise

2.2.2 Each service will follow the containment procedure outlined above and will work alongside the relevant sections where:

- ITS will attempt to limit further access to the information and prevent any further unauthorised access using the same route, if appropriate.
- Estates will secure any affected University building - this may include the repair or replacement of damaged items, changing locks or security access codes, as required.

- Appropriate Senior Officers - with advice from the Data Protection Officer - will assess the impact of the loss/disclosure of business-critical information and take appropriate action in response.

2.2.3 Establish whether or not anything can be done to recover any losses and limit the damage the breach of security can cause. This might include:

- physical recovery of equipment;
- physical recovery of paperwork, where possible (this could include arranging to collect information in person or obtaining written confirmation that the information has been securely destroyed);
- use of backups to restore lost or damaged data;
- alerting staff in the area where the breach occurred, to enable them to recognise when someone tries to use stolen data to access accounts or services.
- stop taking card payments
- Making arrangements with affected individuals to limit any unauthorised access to their information as a result of the security breach e.g. putting passwords on their accounts so they can verify their identity when they contact the University.

2.2.4 Discuss and agree any proposed containment action with SIRO/Deputy SIRO, the University Data Protection Officer and Freedom of Information Officer (Vice Chancellor Office) BEFORE contacting any individuals or agencies concerned, to ensure no further breaches occur.

2.2.5 The police may already have been informed of the incident, but if not a decision by the SIRO/Deputy SIRO will be taken at this point whether to involve them.

3. Risk

3.1 Assessment of on-going risk

3.1.1 Any risk must be accurately defined and assessed in order to maximise the University's ability to control and mitigate the risk.

3.2 Risks from Data

3.2.1 What type of data is involved? Remember that personal data is any information which identifies a living individual and tells you something about them. It does not have to include their name if other information identifies them. This could include;

- Photographs
- Medical information

- Email/IP address
- Financial data (e.g. bank details)
- Personal Identification data (e.g. address, N.I. number)
- University/Graduation year group together with initials etc.

3.2.2 What impact could it have on individuals?

- Is it 'sensitive personal data' as defined by the Data Protection Act, i.e. relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health condition, sexual life, offences committed or alleged, or convictions.[1]
- Is it generally perceived as sensitive because of what might happen if it is misused e.g. bank account details, information that could cause embarrassment to the individual?

3.2.3 Are there any protections in place such as encrypted laptop, USB sticks, secure e- mails etc?

3.2.4 How many people are affected by the incident?

3.2.5 How serious might the effect of the incident on those people be?

- physical risk;
- financial risk;
- identity fraud risk;
- damage to personal reputation;
- negative impact on their privacy;
- damage to organisational reputation;
- disclosure of sensitive personal information.

3.2.6 What is the likelihood of the identified risk occurring?

- For example, if IS equipment is stolen, would someone need very specialist equipment and knowledge to access the information? Is the information formatted in such a way
  e.g. using ID numbers rather than names which would make it harder for individuals to be identified?

3.2.7 Whose data is involved?

- Service users, students or customers?
- Governors?
- Staff or employees of associated bodies?
- Suppliers or partners?

[1] Definition from - ICO website

3.2.8 What are the possible consequences for the University or Governors' reputation (including service delivery)?

3.2.9 Could there be a risk to public health?

4. Notification

4.1 Depending on the incident there may be legal, contractual or sector-specific requirements to notify various parties.

4.2 Notification may assist in security improvements and implementation, as well as risk mitigation.

4.3 An immediate assessment must be made as to whether the data subject (ie. The individuals whose data was involved in the incident) should be notified. This should consider;

- How can notification help the individual?
- Would notification result in undue stress, outweighing the benefit of notifying them?
- Are the individuals who would be notified capable of understanding the notification?
- Are the numbers involved so large that notification would involve disproportionate effort?

As a general rule, it is recommended that the data subject is advised unless you can clearly justify why it is not in the data subject's interest. The SIRO will make the decision and the justifications which will be documented in Section 4 of the Report Form or SIGI Panel Outcome Form.

4.4 You should also consider what advice needs to be provided to individuals to safeguard their information, at the time you notify them e.g. if credit card numbers are involved, they should be advised to contact their card provider.

4.5 If the investigating officer is concerned that an employee may be involved in fraudulent activity, review the financial regulations and obtain advice from the Executive Director of Finance who will make the decision on whether further advice is required.

4.6 Are passport numbers involved? If yes, contact the Identity and Passport Service using the contact details on its website.

4.7 Are National Insurance numbers involved? If so contact Her Majesty's Revenue and Customs (HMRC) using the contact details on its website.

4.8 Should the University insurers be notified? If so or if you are unsure, contact the Insurance team for advice insurance@glyndwr.ac.uk

5. Corrective Action

5.1 The investigation officer should identify immediate corrective action taken and submit the Reporting Form Appendix 1 via e-mail to the Data Protection Officer via dpo@glyndwr.ac.uk

6. SIRO Evaluation and Panel Investigation

6.1 The SIRO Evaluation

6.1.1 Upon receipt of the completed Reporting Form in Appendix 1, the Chair of the Information Governance Committee (SIRO) will then assess the incident and decide whether or not this should be considered by a SIGI Panel.

6.1.2 If the SIRO makes the decision that a panel should meet to assess the incident, the panel will meet as soon as practicable

6.1.3 If the SIRO makes the decision that a panel need not meet to assess the incident, the SIRO will provide justifications on the form in Appendix 1 Section 3.

6.1.4 The IGC will meet on at least a quarterly basis to review previous breaches and near misses

6.2 The Panel Investigation

6.2.1 The Investigating Officer will present their initial findings to the panel, who will then:

- assess the incident and the investigation so far, and
- advise on and co-ordinate any further actions required.

6.2.2 The Panel will consist of the following employees:

- Senior Information Risk Owner **(SIRO)** - currently the Executive Director of Human Resources (Chair)
- **Deputy SIRO s** (in the absence of the SIRO) – *(1 = currently University Solicitor & 2 = currently Director of Strategic Planning & Student Administration)*
- **Director of IS**/his/her representative
- **DPO**
- **FOI Officer**
- **Relevant Dean** or **Director** or his/her representative for the relevant part of the breach

- **Line Manager** of person who is responsible for the breach
- **University Solicitor**
- Any other person deemed appropriate on invitation by the SIRO

6.2.3 **Panel Quorum** = **4** *(to include SIRO/Deputy SIRO, University Solicitor and DPO)*

6.2.4 The role of the Panel is to:

- Review the circumstances of the incident and the action taken so far. This should be set out in an investigation report from the Dean of Faculty / Line Manager or Director of the service area concerned.
- Evaluate the circumstances in which the incident took place (see below)
- Consider whether or not any further action needs to be taken to avoid further breaches or similar incidents occurring.
- Identify any charity law issues arising from the breach.
- Agree an action plan, responsible officers and relevant timescales for implementation of follow-up action.
- Make recommendations even if it is only to reinforce existing procedures
- Determine whether or not the Information Commissioner's Office should be advised of the incident (N.B if significant breach reporting needs to occur within 72 hours)

6.3 Panel Evaluation

6.3.1 The Panel will review whether or not any risk of the breach occurring had been identified prior to the incident and whether or not it was avoidable.

If so:

- Did the incident occur despite existing measures being in place?
- Were current policies and procedures followed? If not, why not?
- In what way did the current measures prove inadequate?
- Had staff received appropriate training and communications in relation to information governance?
- If current procedures and policies were inadequate, how can they be improved e.g. by revision and rewriting?

If not:

- How likely is the incident to recur?
- Could a change to current policies or procedures have prevented or lessened the impact of the incident?
- Do the previous two points in this section indicate that current policies and procedures should be rewritten?

6.3.2 Was the employee aware of current policies and procedures?

- If yes, did they comply?
- If not, why not?
- Carry out checks with IS/HR team relating to policies and procedures read and accepted (did employee complete and pass the mandatory on line training and/or attend other data protection training.

6.3.3 Did this involve deliberate or reckless behaviour by an employee?

- If a deliberate act or reckless behaviour, the panel should inform the Head of HR (Operations & Systems) who will consider whether to manage under the appropriate HR policy. This may result in disciplinary measures, whether suspension of person/s from the work place is appropriate (this may be with immediate effect following notification), prosecution or retraining , which is a matter for HR, taking advice from Legal, and outwith the remit of the SIGI panel

6.3.4 The above points will be used to prepare a presentation to the Panel meeting in order to ensure all aspects are considered. The responses to the questions on the Reporting Form in Appendix 1 will form the decision.

7. Response

7.1 ICO Notification

7.1.1 ICO Notification will be determined and agreed by the panel except in cases of emergency when the SIRO in conjunction with the Vice Chancellor will decide using the current guidance from the ICO, which is available on its website.

7.1.2 If the ICO is to be notified, the ICO breach reporting form (available on the ICO website) should be completed by the SIRO/DPO. Information provided by the investigating officer, the SIGI Panel and any other relevant information should be used to complete the reporting form. The notification to the ICO should include as much information as possible which is pertinent to the incident, particularly focusing on remedial action taken and any measures to be implemented or already in place to prevent the security breach reoccurring. Any action against responsible employees should also be included (within reason, taking account of their reasonable right to privacy) to demonstrate that the University policies and procedures are being implemented and enforced.

7.1.3 Once completed, the Reporting Form in Appendix 1 will be considered by the SIRO and the Vice Chancellor who will authorise the notification to the ICO.

7.1.4 If agreed by SIRO and VC, the form will be sent to the ICO by the Data Protection Officer. The Clerk to the Board of Governors will be notified who will then inform the Chair of the Audit Committee, Chair of the Board of Governors, Charities Commission and HeFCW of the University's notification to the ICO.

7.1.5 The ICO will respond to the breach notification and may conduct further investigations. The findings of the ICO investigation may require further changes to policies or procedures or impose sanctions. Under Part 6 of the Act, there are two tiers of penalty for an infringement of Part 3 - the higher maximum and the standard maximum. These could include a public undertaking to improve compliance and make changes or could involve a fine of up to £8.7 million or 2% (standard maximum) of the University turnover in the preceding financial year, or a more serious breach; £17.5 million or 4% (higher maximum) of the University turnover in the preceding financial year.

7.2 Policy and Procedural Changes

7.2.1 It is recognised that policies and procedures may need to be reviewed as a result of the incident.

7.2.2 If any changes are made as a result of the incident, this should be clearly noted within the policy or procedure concerned.

7.3 Staff Notification and Training

7.3.1 Where policy or procedure changes are introduced, all relevant staff should be informed of the changes and required to record their acknowledgement of reading and understanding the changes.

7.3.2 There may be a requirement to repeat, extend or revise training. All involved staff should be required to undertake any new or repeated training resulting from the incident.

7.4 Recommendations

7.4.1 Regardless of the type and severity of the incident, there will always be recommendations to be made even if it is only to reinforce existing procedures. There are two categories of recommendation that can be made:

- **Local** – these apply purely to the department affected by the incident and will usually reflect measures that need to be taken to restrict the changes of the same type of incident reoccurring
- **Corporate** – some incidents will be caused by factors that are not unique to one Department or Faculty but can be found right across the University. Issues

such as training, information handling and physical security affect all sections of the University and it is essential that the University identifies such risks and puts in place measures to prevent the incident occurring elsewhere.

7.4.2 All recommendations will be assigned an owner and have a timescale by when they should be implemented which has a dual purpose. The first is to ensure that the University puts in place whatever measures have been identified and that there is an individual that can report back to the DPO on progress as requested. The second
is that where incidents are reported to the ICO, the University can demonstrate that the measures have either been put in place or that there is a documented plan to do so.

7.4.3 This is a recurrent theme of ICO enforcement and the UK GDPR doesn't change that, it's important that the University's procedures reflect this. Identifying recommendations is more than just damage control, the knowledge of what has happened together with the impact is a fundamental part of learning which can then by disseminated throughout the University.

7.5 Monitoring

7.5.1 The DPO will monitor the implementation and progress of Action Plans for all incidents and escalate any issues arising to the SIRO/Deputy SIRO.

7.5.2 On the conclusion of an investigation, the information logged by the DPO and included in IG Newsletter updates and awareness articles/lessons learnt in Campus Talk

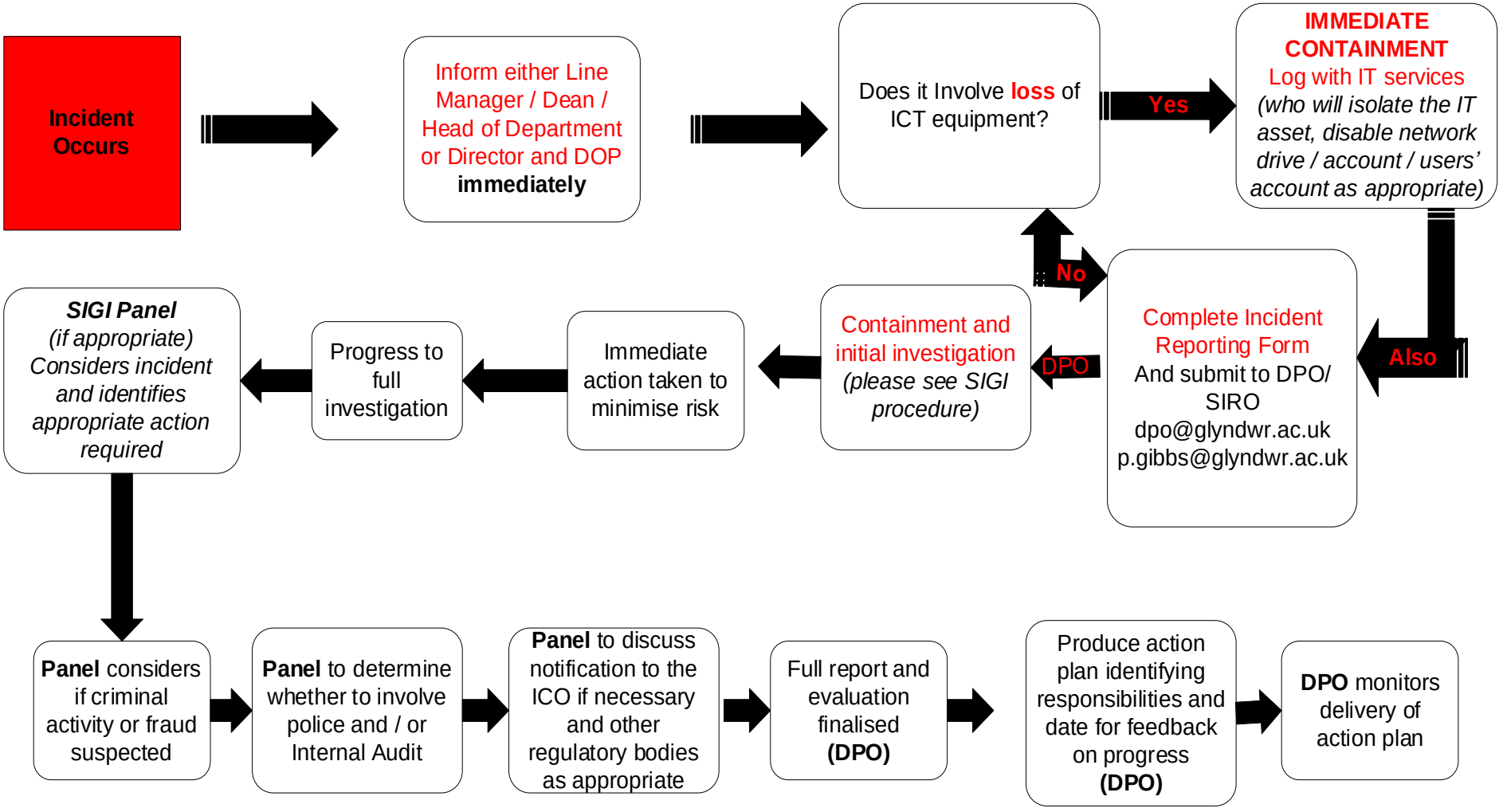
7.5.3 A summary of incidents will be submitted to each IG Committee meeting and a subsequent report from the Information Governance Committee will be submitted to VCET for review.

7.5.4 If further information is required relating to this policy please speak to your Line Manager in the first instance, or the Data Protection Officer via dpo.@glyndwr.ac.uk

8. Summary of Timescales and Responsibilities

Process	Responsibility	Timescale *(from occurrence)*
Reporting	Employee and/or Line Manager of Employee reporting incident	**Immediately**
Containment	Investigating Officer *(liaison with DPO)*	**24 hours**
On-going risk assessment	Investigating Officer *(liaison with DPO)*	**48 hours**
Notificationof affected parties	Investigating Officer *(liaison with DPO)*	**48 hours** *(or immediately if potential security breach)*
ICO Notification	Vice Chancellor Board	**72 hours**
Complete Reporting Form submitted to DPO	Investigating Officer	**1 - 2 working days**
SIGI Panel Review / Evaluation	Senior Information Risk Owner	**ASAP** if SIRO makes decision to convene a panel
Action Plan Agreed	Director/nominated person of area where incident occurred	**1 month** *(may change dependent upon assessment of risk)*
Action Plan Completed	Director/nominated person of area where incident occurred	**1 month** *(may change dependent upon assessment of risk)*
Monitoring	Information Governance Committee	**Monitored quarterly**
Review	VCET	**Annual Report**

9 Overview of SIGI Process



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 as soon as possible.

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

Section 2: Assessment of Severity	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.
Details of the IT systems, equipment, devices, records involved in the IT security breach:	
Details of information loss:	
How much data has been lost? *If laptop lost/stolen: how recently was the laptop backed up onto central IT system?*	
How many data subjects affected?	
Is the data bound by any contractual security arrangements? *E.g. Commercial contracts/data processing agreements.*	
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:**	
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**?	
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**?	
Spreadsheets of **marks** or **grades obtained by students**, **information** about **individual cases of student discipline** or **sensitive negotiations which could affect adversely affect individuals?**	
Security information that would compromise the safety of individuals if disclosed?	

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

Glyndwr University - Information Classification Scale (as referred to in the University's Information Security Policy)

	Public	Open	Confidential and Sensitive (additional conditions and safeguards must be applied for 'special category' – data that can cause harm or distress to an identifiable individual if generally released including on individuals)	Secret
Impact if the information is made public:	**None**	**Low** May result in very minor reputational or financial damage to the University; May result in very minor privacy breach for an individual	**Medium/High** Could substantially damage reputation of the University, Have a substantial financial effect on the University or a third-party, Would result in a serious privacy breach to one or more individuals	**Critical** May damage national security
Definition:	May be viewed by anyone, inside or outside the organisation	Available to people at the University who are in one of other of these groups: 'staff', postgraduate researchers' and 'taught students'	Access is controlled and restricted to a group of people. (These may be people who are members of the University and also people who are members of other organisations) Access is restricted to a small number of people who are listed by name.	Postgraduate researchers who have been explicitly cleared and vetted for access Information shared with 3rd parties e.g. Police
Description:	**Public Information assets may include but are not limited to:** - Publications - Press releases - Course information - Principal University contacts for public facing roles i.e name e- mail address and landline telephone number - Public events N.B. where the incident relates to loss or potential loss of payment card data, then the process outlined in the PCI DSS Incident Response Management Procedure must be followed	**Open information assets may include but are not limited to**: - Contact information for most staff (e.g. name, role, e-mail address and University telephone number) - Policies, procedures and guidelines - Internal University communications - University internal events	**Confidential information assets may include but are not limited to:** -Personal details and identifiable information e.g. name/address/telephone number/email address/date of birth/ passport/IP address -Wage slips -Death certificates -Employee contract information -Non Disclosure Agreement - Student transcripts - Examination papers - Staff/student medical records - certain medical research data - Research papers intended to lead to patentable results (If research is ongoing and has not been published) - Details of servers and server rooms - Passwords - Investigations/disciplinary proceedings - Submitted patents/Intellectual Property Rights -University and third party contract/supplier information -Market sensitive information (e.g. concerning some property purchases) **Special Category and Criminal Conviction Personal Data** - Financial data -National Insurance Number -Bank Details including sort code/account number -Racial or ethical origin -Political opinions -Religious or philosophical beliefs -Trade union membership -Genetic data -Biometric data (where used for identification) -Health -Sex life or sexual orientation -Criminal convictions and offences	Access is subject to or obtained under the Official Secrets Act or equivalent. Access and disclosure pursuant to s.26 Counter Terrorism and Security Act 2015

11 APPENDIX 2

SIGI PANEL OUTCOME FORM

This form is included with papers for panel members to understand format of discussion and is completed by DPO either during or following the meeting.

PANEL IN ATTENDANCE	
DATE:	
INCIDENT LOG NUMBER:	
PANEL RECOMMENDATIONS:	
ACTION PLAN:	
DATE OF ACTION PLAN COMPLETED: **SIGNED:**	

Panel of [*insert date***] @ [***time***] via [***Microsoft Teams/room number***]**

Discussion:

Should the data subjects be informed?

Should the ICO be informed?

Create additional page to continue with notes if required