Data Breach Notification

1. **Introduction**
	1. The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority (ICO for the College). The College must do this within 72 hours of becoming aware of the breach, where feasible.
	2. The College is required to notify Welsh Government within 24 hours of discovering a breach involving any Work-based learning related data.
	3. If the breach is likely to result in a high risk of adversely affecting individuals’ rights and freedoms, the College must also inform those individuals without undue delay.
	4. The College should ensure that it has robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not it needs to notify the relevant supervisory authority and the affected individuals.
	5. The College must also keep a record of any personal data breaches, regardless of whether you are required to notify.
	6. The Protocol for responding to a personal data breach is set out in Appendix 1 below.
2. **What is a personal data breach**
	1. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

2.2 Personal data breaches can include:

access by an unauthorised third party;

deliberate or accidental action (or inaction) by a controller or processor;

sending personal data to an incorrect recipient;

computing devices containing personal data being lost or stolen;

alteration of personal data without permission; and

loss of availability of personal data.

2.3 A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

2.4 Recital 87 of the GDPR makes clear that when a security incident takes place, the organisation should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

**3. What breaches must be notified to the ICO?**

3.1 When a personal data breach has occurred, the College needs to establish the likelihood and severity of the resulting risk to people’s rights and freedoms. If it’s likely that there will be a risk then it must notify the ICO; if it’s unlikely then it doesn’t have to be reported. However, if the College decides that it doesn’t need to report the breach, it needs to be able to justify this decision, so it should be documented.

3.2 In assessing risk to rights and freedoms, it’s important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

*“A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.”*

3.3 This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. This needs to be assessed on a case by case basis, looking at all relevant factors.

**4. What information must a breach notification to the ICO contain?**

4.1 When reporting a breach, the GDPR says the College must provide:

* a description of the nature of the personal data breach including, where possible:
	+ - the categories and approximate number of individuals concerned; and
		- the categories and approximate number of personal data records concerned;
* the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
* a description of the likely consequences of the personal data breach; and
* a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

**5. What if all the required information is not available yet?**

5.1 The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So Article 34(4) allows for the organisation to provide the required information in phases, as long as this is done without undue further delay.

5.2 However, the ICO expects controllers to prioritise the investigation, give it adequate resources, and expedite it urgently. The College must still notify the ICO of the breach when it becomes aware of it, and submit further information as soon as possible. If it knows that it won’t be able to provide full details within 72 hours, the College will need to explain the delay to the ICO and tell them when we expect to submit more information.

**6. When do individuals need to be informed of a breach**

6.1 If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says that those concerned must be informed directly and without undue delay. In other words, this should take place as soon as possible.

6.2 A ‘high risk’ means the threshold for informing individuals is higher than for notifying the ICO. Again, the College will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, the College will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

6.3 If the College decides not to notify individuals, it will still need to notify the ICO unless it can demonstrate that the breach is unlikely to result in a risk to rights and freedoms. The ICO has the power to compel the College to inform affected individuals if it considers there is a high risk. In any event, the College should document the decision-making process in line with the requirements of the accountability principle.

Appendix 1

Protocol

1. Identify a breach
2. Contain the breach
3. Notify the DPO as soon as possible at dpo@gowercollegeswansea.ac.uk
4. DPO to investigate the breach in consultation with relevant staff members (Business Continuity Team?)
5. DPO to assess using ICO guidance, and in consultation with data owners the likelihood and severity of the resulting risk to people’s rights and freedoms and determine:
	1. whether to notify the ICO (Draft Appendix 2)
	2. whether to notify individual (Draft Appendix 3)
6. DPO to notify ICO of the breach via website or telephone call without undue delay and within 72 hours or provide explanation if there is a delay
7. DPO to notify individuals
8. Where DPO is the processor of the data to notify controller as soon as possible
9. Record breach (Appendix 4)
10. Report to Audit Committee

Appendix 2

Draft Breach notification letter to ICO

Dear [ICO]

By way of this communication, Gower College Swansea is reporting a data breach involving [number of people/records] that occurred on [date of incident]. The categories of personal data involved in this data breach are [categories of data involved]

[Name of Data Protection Officer] is the Data Protection Officer for Gower College Swansea. S/he can be contacted at [contact details].

Because of this breach, [describe likely consequences]. We intend to take the following action and mitigate the damages caused by this breach [explain what action will be taken].

Yours sincerely

DPO

 Appendix 3

Draft Breach notification letter to individuals

Dear [individual name],

We are writing to inform you that on [date] we experienced a [hacking/loss of data/accidental loss etc. or other type of breach]. Unfortunately, your [state categories of data] was [lost/stolen/potentially exposed/disclosed]. We have [describe the action taken to contain the breach] and believe that [outcome – data secure/problem solved].

The College Data Protection Officer is [name] and s/he can be contacted at [contact details].

The College takes data security extremely seriously and we apologise for any inconvenience this may cause.

Yours sincerely

DPO

Appendix 4

Breach Register

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Breach Description** | **Date of breach** | **Breach Effect** | **Remedial Action Taken** | **Date of remediation** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |