Document Name and Version	**10.5 Data Breach Policy**
Policy Number	10.5
Policies that Interact with 10.4	10.1 Data Policy; 10.2 Data Protection Processing Principles 10.3 Data Management and Retention Policy; 10.4 Data Breach Policy; 10.6 Webpage Privacy and Cookie Notice; 10.7 Your Right of Access to Personal Information held by IICP College;
Approval Body	Board of Directors
Date of Approval	February 2020
Date Policy Comes into Force	25th January 2021
Date of Review	2025
Revisions	

1. Preamble.

1.1. This is a Personal Data Breach Policy, which sets out the procedures to be followed in IICP College in order to prevent personal data stored or processed by the College being subject to a breach, and the procedures to be followed in the event of a breach.

2. Purpose.

2.1. The policy is designed to aid compliance with the General Data Protection Regulation [GDPR].

2.2. This policy takes account of the Data Protection Commission Guidance on Data Breach[1] and Article 29 of the Data Protection Working Party's guidance on personal data breach notifications[2]. The Working Party's guidance encourages organisations to:

> "plan in advance and put in place processes to be able to detect and properly contain a breach, to assess the risk to individuals, and then to determine whether it is necessary to notify the competent supervisory authority, and to communicate the breach to the individuals concerned when necessary" (p. 5).

2.3. This policy aims to ensure that adequate controls are in place so that:

- Data breaches are identified, and action is taken quickly. Actions should be proportionate, consistent and transparent;
- An assessment is completed to ensure that any major data breaches are reported to the Senior Management Team (SMT) and Data Protection Contact (DPC);
- All data breaches and near misses are recorded and regularly reported as appropriate;
- Lessons are learnt to ensure similar mistakes are not repeated and appropriate control mechanisms are put in place.

2.1 This policy addresses the following legislative and regulatory requirements:

---

[1] Data Protection Commission. (2018) *New: Breach Notification Process Under GDPR* Available at: https://dataprotection.ie/docs/GDPR-Overview/m/1718.htm (Accessed 27 October 2018).

[2] Article 29 Working Party. (October, 2017) *Guidelines on Personal data breach notification under GDPR.*

- General Data Protection Regulation [GDPR].
- QQI Sector-Specific Quality Assurance Guidelines for Independent/ Private Providers: Management of legislative and regulatory compliance.

3. Scope.

3.1. This policy focuses upon personal data breaches, not information security incidents generally. The policy is not designed for use in relation to any non-GDPR data breach notification arising from contractual, professional or other commitments.

3.2. This policy covers all personal data breaches under the GDPR. A Data Breach is defined by the GDPR[3] in Article 4(12) as:

> "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed by the company".

4. Roles and Responsibilities.

4.1. The Board of Directors is responsible for formally approving this policy and for overseeing its implementation.

4.2. The Senior Management Team is responsible for the scheduling and implementation of staff and learner training requirements for the implementation of this policy and related Data Protection policies.

4.3. The Data Protection Contact is responsible for the operation of this policy and for the creation and implementation of associated policies and procedures.

4.4. All staff are responsible for implementing this policy.

5. Policy.

5.1. This policy is in place to raise awareness of data breach cases, and to ensure that all staff can identify a case and understand the steps required for dealing with them. Therefore, all staff are required to be familiar with this policy.

[3] The full text of the GDPR (Regulation (EU) 2016/679 (General Data Protection Regulation)) can be found here: https://gdpr-info.eu/

5.2. This policy identifies inherent risk of a data breach and/or near-miss, which will ensure that appropriate senior manager and the Data Protection Contact [DPC] are informed, able to manage actions relating to any real or potential serious data breach and are in a position to report to the DPC and affected individuals as appropriate.

5.3. Identifying data breaches quickly and effectively to limit any impact is critical to GDPR. In addition, IICP College is mindful of its responsibility to understand where there are difficulties within operating processes and continuously improve to reduce the risk of data breaches.

5.4. A personal data breach may mean that someone outside IICP College gets unauthorised access to personal and/or special category (sensitive) data. A personal data breach can also occur if there is unauthorised access within the College, such as an employee accidentally or deliberately altering or deleting personal data.

5.5. A data security breach can happen for many 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;
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

5.6. Human error is the most common cause of data breaches. These can happen for many reasons including (but not confined to):

- Theft or loss of paperwork;
- Data posted to incorrect recipient;
- Data sent by email to incorrect recipient;

- Failure to redact personal/sensitive data.

6. Procedures

6.1. *Near misses*:

6.1.1. A near miss is an event that does not result in a data breach, but which had the potential to do so. Examples of such events might include data that was misplaced but found quickly internally or data that was sent out but was identified and returned.

6.1.2. IICP College is committed to identifying weaknesses in our operational procedures. To this end it will record all near misses in order to understand patterns, learn lessons and implement improvements.

6.2. *Identification*:

6.2.1. Data breaches or near misses may be identified as part of everyday business. They may be identified at the first point of contact by a staff member or learner, or by a third party.

6.2.2. Where a data breach is identified the Senior Management Team and the Data Protection Contact (DPC) must be informed immediately. The DPC will investigate the occurrence and complete a risk assessment (see section 5.3) to determine the notification requirements.

6.2.3. The controls in place should be reviewed once a data breach or near miss is identified. Where no controls are in place, consideration must be given to introducing them. The test here is: was this an exceptional case that could not have reasonably been avoided, or does action need to be taken to avoid a recurrence?

6.3. *Risk Assessments:*

6.3.1. When a data breach is identified, a risk assessment should be completed.

6.3.2. The DPC will report all incidents to the Senior Management Team.

6.3.3. The DPC will provide advice and guidance on managing the containment and recovery of any lost data and will support the investigation process.

6.3.4. The Senior Management Team in consultation with the DPC will decide how best to deal with the case, with particular reference to containment and recovery, the investigation process and notification requirements.

6.4. *Containment and recovery*:

6.4.1. Containment and recovery involve limiting the scope and impact of the data breach, and stemming it as quickly as possible.

6.4.2. The DPC, in consultation with Senior Management, must take appropriate steps to ascertain full details of the breach, determine whether the breach is still occurring, recover any losses, and limit the damage.

6.4.3. The steps might include:

- Attempting to recover any lost equipment or personal information;
- Shutting down an IT system;
- Contacting key departments so that they are prepared for any potentially inappropriate enquiries about the affected data subjects;
- Organising, with the approval of the Senior Management Team, for appropriate notifications;
- The use of back-ups to restore lost, damaged or stolen information;
- Where bank details have been lost/stolen consider contacting banks directly for advice on preventing fraudulent use;
- If the data breach includes any entry codes or passwords then these codes must be changed immediately, and the relevant organisations and members of staff informed.

6.5. *Investigation:*

6.5.1. If a data breach is identified, then a formal investigation should be commenced by the DPC. The investigation aims to ensure that the case is being managed and any improvement actions agreed are implemented. The investigation should be proportionate to the breach identified and risk of harm.

6.5.2. The DPC should determine the seriousness of the breach and the risks arising from it. Specifically, the following should be identified:

- Whose information was involved in the breach;

- What went wrong;
- The potential effect on the data subject(s);
- What immediate steps are required to remedy the situation;
- What lessons have been learnt to avoid a repeat incident.

6.5.3. In determining the seriousness of the breach, the investigation should consider:

- The type of information;
- Its sensitivity;
- The individuals affected by the breach, and the number of individuals involved;
- What protections are in place (e.g. encryption);
- What happened to the information;
- Whether the information could be put to any illegal or inappropriate use;
- What the information could tell a third party about the individual;
- Whether those affected have any special needs/vulnerabilities.

5.5.4 The initial investigation should be completed urgently. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

6.6. *Notifications:*

6.6.1. The decision regarding notification lies with the Senior Management Team. The DPC needs to take into account when producing this report that the time limit for notification of the Data Protection Commission is 72 hours.

6.6.2. There are two different types of notification that should be considered:

6.6.2.1. Notifications by a data controller to the supervisory authority, the Data Protection Commission;

6.6.2.2. Notifications by a data controller to data subjects, i.e. the people whose data has been breached. This should be carried out on a case by case basis, taking into account the data subjects involved, the level of threat and the consequences to all involved.

6.6.3. Notifications by a data controller to the Data Protection Commissioner.

6.6.3.1. A breach that occurs in circumstances where the College considers that the breach presents a risk to individuals must be reported to the Data

Protection Commission [DPC]. Breaches must be reported to the DPC, typically within 72 hours, unless the data was anonymised or encrypted. In practice this will mean that most data breaches must be reported to the DPC. Breaches that are likely to bring harm to an individual – such as identity theft or breach of confidentiality – must also be reported to the individuals concerned.

6.6.3.2. Notification should be on the DPC form, which is available at https://www.dataprotection.ie/documents/gdpr_forms/National_Breach_Notification_Form.pdf . A copy is reproduced below (section 6).

6.7. *Informing affected individuals:*

6.7.1. The College is required to inform those affected where there is a significant breach of personal and sensitive data and the risk of harm to those individuals is high.

6.7.2. If there is a high risk of further harm, then the College has an obligation to disclose the breach to each individual affected.

6.7.3. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

6.8. Learning lessons:

6.8.1. A "Lessons Learnt" Action Plan for data breaches and near misses should be completed.

6.8.2. The Action Plan should clearly outline the lessons learnt, the controls agreed to reduce the risk of a further reoccurrence, who is responsible for this implementation and a completion date.

6.8.3. The case will not be considered closed until all actions agreed have been completed.

6.8.4. It is envisaged that this should be completed within 10 working days of the data breach being identified.

6.9. *Data Breach Log*:

6.9.1. All data breaches, including near misses, will be recorded on a data breach log. All issues identified by the application of this policy will be recorded in the data breach log and categorised according to whether it is a data breach or near miss.

6.9.2. This information will be reviewed and analysed on a regular basis to identify patterns and monitor the implementation of agreed service improvements.

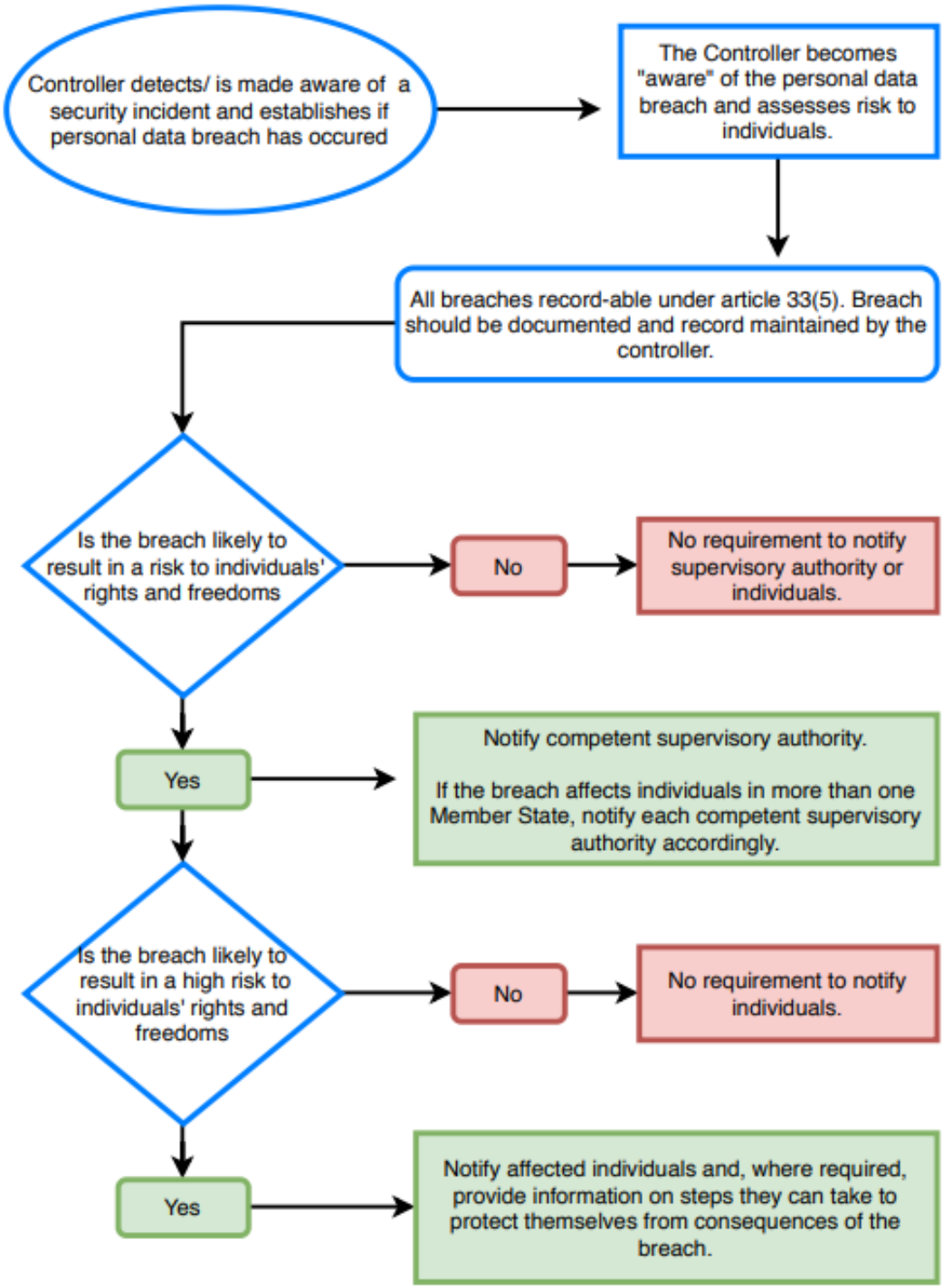
6.9.3. The Data Protection Contact [DPC] will collate all data breach reports and will report trends and lessons learnt quarterly to the Board.

7. Supporting documentation.

7.1. The following form is provided by the Data Protection Commissioners for use in notification of a breach. Please use the latest online form available at: https://www.dataprotection.ie/documents/gdpr_forms/National_Breach_Notification_Form.pdf

7.2. The following guidance on notification is given by Article 29 Data Protection Working Party[4] (Available at ec.europa.eu/newsroom/document.cfm?doc_id=47741).

[4] Article 29 Data Protection Working Party. *Guidelines on Personal data breach notification under Regulation 2016/679*. Available at: ec.europa.eu/newsroom/document.cfm?doc_id=47741 (Accessed 27 October 2018).


Controller detects/ is made aware of a security incident and establishes if personal data breach has occured
The Controller becomes "aware" of the personal data breach and assesses risk to individuals.
All breaches record-able under article 33(5). Breach should be documented and record maintained by the controller.
Is the breach likely to result in a risk to individuals' rights and freedoms
No
No requirement to notify supervisory authority or individuals.
Yes
Notify competent supervisory authority.
If the breach affects individuals in more than one Member State, notify each competent supervisory authority accordingly.
Is the breach likely to result in a high risk to individuals' rights and freedoms
No
No requirement to notify individuals.
Yes
Notify affected individuals and, where required, provide information on steps they can take to protect themselves from consequences of the breach.