Personal Data Breach Response Plan

What is a personal data breach?

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 transmitted, stored or otherwise processed.

Internal notification

Any actual or suspected personal data breach, or that data has been placed at risk, is to be notified the DPO immediately. This includes a breach notification sent to Carlow College by any processor, joint controller or collaborative partner.

You must ensure that the DPO receives the information. If you do not succeed in contacting the DPO, contact the President's Office or the Director of Operations. Again, you must ensure that the information has been received.

Assessment of situation

An assessment into the circumstances of the reported breach will commence as soon as possible. The scale of an assessment will be influenced by the situation.

Normally, the assessment team will include the President, the Director of Operations and the DPO. Other employees may join the assessment team depending on the circumstances. The DPO will advise the assessment team.

The assessment team will determine:

- Whether a breach has occurred;
- The nature of the personal data involved (including whether it includes special categories of personal data);
- The cause of the breach;
- Establish whether there is anything that can be done to recover a loss or contain further loss. This may involve engaging the services of contractors/processors;
- The number of individuals who are affected;
- The potential risk to affected individuals.

The results of the assessment will determine what notifications and further actions are required, if any. Complex, large-scale breaches will require thorough investigation. An Garda Síochána will be notified in cases involving criminal activity.

Notifying a personal data breach to the Office of the Data Protection Commission (DPC)

Controllers have a mandatory obligation to report data breaches to their supervisory authority (the DPC) within 72 hours of becoming aware of a breach, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.

When a controller notifies a breach to the DPC, it should, at the minimum:

- Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
- Communicate the name and contact details of the DPO or other contact point where more information can be obtained;
- Describe the likely consequences of the personal data breach;
- Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The controller should also inform the DPC if it intends to provide more information at a later point. The DPC may request further details of part of its investigation into a breach. The DPC is empowered to require controllers to inform data subjects about the breach.

If notification is not made within 72 hours, a reasoned justification for the delay must be provided. The 72 hours does not take weekends, public holidays etc into account. Awareness begins when the controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.

Notifying personal data breaches to data subjects

Controllers have to notify data subjects where the data breach is likely to result in a 'high risk' to affected data subjects. WP29 (now the European Data Protection Board; hereafter EDPB) advice is that 'high risk' exists when the breach may lead to physical, material or non-material damage for the individuals whose data has been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves personal data that involves racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offended or related security measures, the breach should be considered high risk.

Notification to data subjects is not required where:

- The controller has implemented appropriate technical and organisational measures that render the personal data unintelligible to anyone not authorised to access it, such as encryption; or
- The controller has taken subsequent measures which ensure that the high risk to data subjects is not likely to materialise; or
- It would involve disproportionate effort, in which case there should be a public communication instead.

In the event that Carlow College informs data subjects of a data breach, the most appropriate method will depend on the circumstances. In general, data subjects must be contacted by some personally directed method rather than a general public notice.

Notification may be by telephone call, SMS, email or letter. Public notices may also be posted on the College website or social media accounts.

When notifying data subjects of a breach, the controller should provide the following information, at least:

- A description of the nature of the breach;
- The name and contact details of the DPO or other contact point;
- A description of the likely consequences of the breach; and
- 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.

Where appropriate, specific advice should be given to data subjects to protect themselves from possible adverse consequences of the breach, such as resetting passwords where access credentials have been compromised.

At the request of the President, the Marketing Office may assist in communicating with data subjects and responding to any media queries.

Required actions when Carlow College is a processor

Carlow College is a processor in terms of some its data processing. Processors have to notify controllers of breach situations. WP29 (now the EDPB) guidance is that processors notify controllers immediately, with further information about the breach provided in phases as information becomes available. Notifications to controllers will be in writing.

The DPO will act as a point of contact for controllers at the request of Carlow College. Data sharing agreements may impose a timeframe for notification to controllers.

Review of response to breach

In the aftermath of a personal data breach, a review of the incident may take place to ensure both that the steps taken during the incident were appropriate and effective, and to identify any organisational or technical measures that require updating to minimise future risk of a similar incident.

Register of breaches

Controllers must keep an internal record of all data breaches, a description of the facts of the breach, its effects and the remedial action taken. The record should also include reasoning for decisions taken in response to a breach. In particular, if a breach is not notified, a justification for that decision should be documented. This should include reasons why the controller considers that

the breach is unlikely to result in a risk to the rights and freedoms of individuals. The DPO will keep this record on behalf of Carlow College.