Loreto Secondary School, Wexford.

Personal Data Security Breach Code of Practice

Controller:	Loreto Secondary School, Wexford
Address:	Pembroke Hill, Ballynagee, Wexford
Contact:	Email: n.goggin@loretowexford.com Phone: +353 (0)53 91 46162
Privacy Coordinator:	Noeleen Goggin
Approved by Board of Management on:	
Policy became operational on:	
Next review date:	

CONTENTS

Overview

Loreto Secondary School, Wexford (also referred to in the policy as "the school") is required under the General Data Protection Regulation 2016/679 and the Data Protection Act 2018 to safeguard the security and confidentiality of the personal information/data it holds on behalf of its students, staff, parents and any other relevant data subjects. It is important to our school that any suspected data breaches are responded to promptly so as to limit the risk of harm to individuals whose data we hold as well as avoiding any risk of operational or reputational damage to the school.

Purpose

The purpose of this procedure is to provide a framework for reporting and managing personal data breaches affecting any personal data held by the school. This procedure supplements the school's Privacy Policy which affirms its commitment to protecting the privacy rights of individuals in accordance with Data Protection legislation.

What is a personal data breach?

Article 4(12) GDPR defines a 'personal data breach' 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".

Loreto Wexford may suffer a breach for a number of reasons including:

- the disclosure of confidential data to unauthorised individuals;
- improper disposal of documents;
- loss or theft of data or equipment on which data is kept;
- loss or theft of paper records;
- inappropriate access controls allowing unauthorised use of information;
- suspected breach of Loreto Wexford IT security;
- attempts to gain unauthorised access to computer systems, e.g. hacking;
- viruses or other security attacks on Loreto Wexford IT systems or networks;
- breaches of physical security;
- breach as a result of third party breach;
- confidential information left unlocked in accessible areas; and
- emails containing personal or sensitive information sent in error to the wrong recipient.

Who does this procedure apply to?

This procedure applies to:

- The Loreto Wexofrd school
- All staff and volunteers of Loreto Wexford
- All contractors, suppliers and other people working on behalf of Loreto Wexford

What types of data does this procedure apply to?

This procedure applies to:

- all personal data created or received by the Loreto Wexford in any format;
- personal data held on all Loreto Wexford IT systems; and
- any other IT systems on which Loreto Wexford data is held or processed.

Procedure for reporting personal data breaches

In the event of a breach of personal data occurring, it is vital to ensure that it is dealt with immediately and appropriately to minimise the impact of the breach and prevent a recurrence. If a staff member, committee member or Board member becomes aware of an actual, potential or suspected breach of personal data, he/she must report the incident to the Privacy Coordinator immediately.

The Privacy Coordinator must then:

- report the incident immediately the Principal
- record the breach in the school's internal breach register and then follow the procedures outlined further in this document

This will enable all the relevant details of the incident to be recorded consistently and communicated on a need-to-know basis to relevant staff so that prompt and appropriate action can be taken to resolve the incident.

Procedure for managing data breaches

In the event of a breach occurring, the subsequent breach procedure will be adhered to under 5 main headings:

- Identification and Classification
- Containment and Recovery
- Risk Assessment
- Notification of Breach
- Evaluation and Response

It is important to remember that time is of the essence when it comes to data breaches as the school only has 72 hours from when it becomes aware of a breach to notify the Data Protection Commission (DPC) where such notification is required.

Breaches can be categorised according to the following principles, with examples being given:

(i) Confidentiality – an unauthorised or accidental disclosure of, or access to, personal data.

(ii) Integrity – an unauthorised or accidental alteration of personal data.

(iii) Availability – unauthorised or accidental loss of access to, or destruction of, personal data e.g. deletion of data accidentally or by an unauthorised person or unavailability due to a power failure or service attack.

It is important to note that an availability breach may occur even if data is only temporarily lost or unavailable, although such a breach may not need to be notified unless it is likely to result in a risk to the rights of individuals in the given circumstances.

Identification and Initial Assessment

As soon the Privacy Coordinator is made aware of the breach, an initial assessment will be carried out to determine the following:

- if a personal data security breach has taken place; if so:
- what personal data is involved in the breach;
- the cause of the breach;
- the extent of the breach (how many individuals are affected);
- the harms to affected individuals that could potentially be caused by the breach;
- how the breach can be contained.

Contracted companies operating as data processors: Where an organisation contracted and operating as a data processor on behalf of the school becomes aware of a risk to personal/sensitive personal data, the organisation will report this directly to the school as a matter of urgent priority. In such circumstances, the principal of the school should be contacted directly. This requirement is clearly set out in the school's data processing agreements.

Containment and Recovery

Once it has been established that a breach has occurred, the following actions will be carried out:

1. The Privacy Coordinator will control the investigation.

2. Establish who needs to be alerted and what they are expected to do. Where data has been "damaged" (as defined in the Criminal Justice Act 1991, e.g. as a result of hacking), the matter must be reported to An Garda Síochána. Failure to do so will constitute a criminal offence in itself ("withholding information") pursuant to section 19 Criminal Justice Act, 2011. Depending on the nature of the personal data at risk and particularly where sensitive personal data may be at risk, the assistance of An Garda Síochána should be immediately sought. This is separate from the statutory obligation to report criminal damage to data arising under section 19 Criminal Justice Act 2011 as discussed at (2) above. In addition, and where appropriate, contact may be made with other bodies such as the HSE, financial institutions etc.

3. Decide on whether or not there is anything that can be done to limit the damage caused by the breach or recover any lost information. Depending on the nature of the threat to the personal data, this may involve a quarantine of some or all PCs, networks etc. and requesting that staff do not access PCs, networks etc. Similarly, it may involve a quarantine of manual records storage area/s and other areas as may be appropriate. By way of a preliminary step, an audit of the records held or backup server/s should be undertaken to ascertain the nature of what personal data may potentially have been exposed.

4. Establish if it is appropriate to notify affected individuals immediately (e.g. where there is a high level of risk of serious harm to individuals). This analysis is carried out on a case by case basis and is covered under "Risk Assessment".

5. Consult any relevant external advisers such as IT consultants regarding appropriate action where necessary; and

6. Enter the full details of the breach, its effects and remedial action taken into the breach register.

Risk Assessment

In assessing the risk arising from the breach, consideration will be given to what would be the potential adverse consequences for individuals, to do this the following will be considered:

- The type of breach;
- The nature of information/data involved;
- The sensitivity of the information/data;
- The severity of consequence for individuals;
- The special characteristics of the individual(s) – e.g. a breach affecting vulnerable individuals may place them at a greater risk of harm;
- The number of individuals affected by the breach;
- Any security mechanisms in place (e.g. password, encryption) that would prevent individuals being identified;
- What could the information/data convey to a third party about the individual?

The findings of the risk assessment will determine what action should be taken.

Notification of Breach

On the basis of the evaluation of risks and consequences, it will be determined whether it is necessary to report the breach to other parties outside the school.

If the school decides that it is necessary to notify the Data Protection Commissioner (DPC), this must be done within 72 hours of being made aware of the breach.

The details that are needed for the breach notification to the DPC include:

- The contact details for the Privacy Coordinator or designated lead;
- The date and time the breach occurred;
- The date and time the school became aware of the breach;
- The cause of the breach;
- What took place;
- Is the breach on-going;
- What type of personal data that were affected;
- The number of data subjects affected by the breach;
- Whether the data subject/s affected have been contacted;
- The effects and consequences of the breach;
- The mitigating action taken; and

- The remedial action now required.

The school needs to decide whether the risk to the individuals whose data was breached constitutes a high risk their rights and freedoms. If it is decided that the breach could cause either material or non-material damage to the individuals, then they will also be notified by means of a dedicated email or a letter, whichever is deemed most appropriate.

There is no specified time frame for notification to the individuals, but the Regulation states that this must be done "without undue delay". The main objective of notification to individuals is so as to give them the opportunity to protect themselves from any negative consequences resulting from the breach.

The notification to the individual/s should include:

- A description of the breach;
- The contact details of the point of contact in Loreto Wexford;
- Any details available about the consequences of the breach; and
- Details of what steps Loreto Wexford will now take to address the breach.

To download the National Breach Notification Form, logon to the DPC website by going to: https://dataprotection.ie/docs/Breach-Notification-Form/m/1726.htm

Please read the Form Guidance prior to completing the Notification Form and then send the completed form to breaches@dataprotection.ie

Evaluation and Response

The full details of the incident will be entered in the school's internal breach register and subsequent to any data security breach, consideration will be given to:

- What action needs to be taken to reduce the risk of future breaches and minimise their impact?
- Whether policies and procedures need to be amended to increase the effectiveness of the response to the breach?
- Are there weak points in security controls that need to be strengthened?
- Are all employees cognisant of their responsibilities for information security and adequately trained?
- Is additional investment required to lessen exposure and if so what are the resource implications?

Depending on the nature of the incident, the Office of the Data Protection Commissioner may investigate the circumstances surrounding the personal data security breach. Investigations may include on-site examination of systems and procedures and could lead to a recommendation to inform data subjects about a security breach incident where the school has not already done so. If necessary, the Commissioner may use the enforcement powers of the office to compel appropriate action to protect the interests of data subjects.

Enforcement

Employees who intentionally do not disclose a personal data breach to the Privacy Coordinator, may be subject to disciplinary action, including suspension and dismissal.

Loreto Wexford reserves the right to update or amend this policy as required.