

<hr/> <p><i>Policy Title & Ref Number</i></p> <hr/>	<p>Personal Data Breach Policy</p> <p><i>Doc Ref: DP-019</i></p> <p><i>Final v0.1</i></p>
<hr/> <p><i>Policy Prepared By</i></p> <hr/>	<p>Data Protection & Information Compliance Officer</p>
<hr/> <p><i>Policy Owner</i></p> <hr/>	<p>Corporate Services</p>
<hr/> <p><i>Consultation Process</i></p> <hr/>	<p>Management Team</p> <p>SEO Group</p>
<hr/> <p><i>Policy Approved by & Date of Approval</i></p> <hr/>	<p>Management Team</p> <p>12th May 2020</p>
<hr/> <p><i>Review Date</i></p> <hr/>	<p>May 2021</p>

Policy Revision History

<i>Date</i>	<i>May 2020</i>
<i>Revision Details</i>	Original
<i>Implementation Date</i>	19 th May 2020

Purpose of this Policy

The purpose of this Personal Data Breach Policy is to outline Longford County Council's commitment:

- To protecting and safeguarding the personal data held by the Council and
- To ensure appropriate technical and organisational arrangements are in place to fulfil our Data Protection obligations in dealing with instances of personal data breaches or potential personal data breaches

Scope

The scope of this document applies to all Longford County Council employees.

Applicability

This policy applies to all personal data held by Longford County Council and third-party processors, both in physical and electronic format relating to members of the public, customers, suppliers, employees and elected members.

Commencement

This policy shall commence on 19th May 2020



Policy

It is the policy of Longford County Council to protect and safeguard the personal data we collect and process and to ensure as far as is reasonably practicable appropriate technical and organisational measures are in place to protect the personal data.

Definitions

Personal Data Breach is a breach of security leading to the, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to any or all personal data transmitted, stored or otherwise processed by Longford County Council and third-party processors.

Personal Data is any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means such as collection, recording, organising, structuring, storage, adaptation or alteration, retrieval, consultation on, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of the processing of personal data, where the purpose and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law

Third Party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor are authorised to process personal data

Supervisory Authority means an independent public authority which is established by a member state and is responsible for monitoring application of the General Data Protection Regulation in order to protect the fundamental rights and freedoms of natural persons in relation to data processing

Legislative Requirements

It is Longford County Council's policy to ensure that in the event of a personal data breach, that appropriate measures exist to facilitate the identification, containment/recovery, assessment, notification and evaluation of a Personal Data Breach in order to protect the privacy of individuals and to comply with Data Protection Legislation.

1. Identification

If an employee of Longford County Council considers that a personal data breach has or may have occurred, this shall be reported immediately to their line manager **and** the Data Protection & Information Compliance Officer.

2. Containment/Recovery

The reporting employee, Line Manger and the Data Protection & Information Compliance Officer shall establish whether there is anything that can be done immediately to contain and/or recover any losses and limit the damage that the personal data breach is likely to cause.

3. Assessment

Failure to adequately assess risk or failure to attempt to assess risk of a Personal Data Breach may result in Longford County Council failing to meet its obligations under GDPR. Longford County Council are required to notify the Supervisory Authority of a personal data breach, unless the Council can demonstrate that it is unlikely to result in a risk to the rights and freedom of data subjects.

4. Notification

Personal Data Breaches that result in a risk to the rights and freedom of a data subject shall be reported by the Council's Data Protection & Information Compliance Officer to the Supervisory Authority without undue delay and where feasible **within 72 hours** of Longford County Council becoming aware of the breach

Where it is not possible to provide all the information to the Supervisory Authority, the information may be provided in phases without undue delay.

Where a personal data breach takes place in another member state, the Council's Data Protection & Information Compliance Officer shall notify the lead supervisory authority in that member state where the personal data breach occurred and the Data Protection Commission.

Notification of a personal data breach to the Supervisory Authority shall include the following;

- The nature of the breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned.
- The name and contact details of the Data Protection & Information Compliance Officer where more information can be obtained;
- The likely consequences of the personal data breach
- The measures taken or proposed to be taken by the Council to address the personal data breach, including where appropriate, measures to mitigate its possible adverse effects.

In the case of a personal data breach where Longford County Council are the Data Processor, the Council's Data Protection & Information Compliance Officer shall notify the Data Controller as soon the Council become aware of the personal data breach.

The Data Protection & Information Compliance Officer shall, without undue delay, inform the Data Subjects affected by the personal data breach if it is likely to result in a risk to their rights and freedom of the Data Subject(s).

Notification of a personal data breach to the Data Subject shall include the following;

- The name and contact details of the Data Protection & Information Compliance Officer where more information can be obtained;
- The likely consequences of the personal data breach
- The measures taken or proposed to be taken by the Council to address the personal data breach, including where appropriate, measures to mitigate its possible adverse effects.

Longford County Council are **not required** to contact the affected Data Subjects if:

- Appropriate technical and organisational measures to protect personal data were in place prior to the breach which rendered the personal data unintelligible to any person who is not authorised to access it
- Immediately following a personal data breach, the Council takes steps to ensure that the high risk posed to the affected individuals rights and freedom is no longer likely to materialise
- It would involve disproportionate effort to contact individuals, in certain scenarios such as where their contact details were lost because of the breach
- It shall obstruct official or legal inquiries, investigations or procedures, the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, the protection of public security or the protection of national security

5. Evaluation

Following any personal data breach, the Data Protection & Information Compliance Officer long with the Line Manager shall carry out a thorough review of the breach.

Longford County Council shall ensure all steps taken during the personal data breach were appropriate and identify any areas that may need to be improved. All reportable and non-reportable personal data breaches shall be recorded by the Council's Data Protection & Information Compliance Officer on the Council's Data Breach Register.

Responsibilities

Management Team

- Ensure Longford County Council have in place appropriate safeguards and approved organisational policy and procedures to protect all personal data held by Council.

Senior Officers

- Implement the requirements of this policy.
- Contribute to policy development and review where appropriate
- Co-operate fully with all measures being taken to address a personal data breach
- On discovering of a personal data breach or suspected personal data breach inform their line manager **and** Longford County Council's Data Protection & Information Compliance Officer and complete the Council's internal Data Breach Report (Appendix 1).
- Assist and advise employees in their area of responsibility as necessary to ensure that the requirements of this policy are implemented
- Attend and participate in training as required

Line Managers

- Familiarise themselves with the requirements of this policy
- Co-operate fully with all measures being taken to address a personal data breach
- Assist and advise employees in their area of responsibility in its implementation
- Ensure that the requirements of this policy are complied with by employees in their area of responsibility
- On discovering a personal data breach or suspected personal data breach inform their line manager **and** Longford County Council's Data Protection & Information Compliance Officer and complete the Council's internal Data Breach Report (Appendix 1).
- Attend and participate in training as required

Employees

- Familiarise yourself and comply with the requirements of this policy.
- Seek advice or guidance
- Attend and participate in training as required
- Co-operate fully with all measures being taken to address a personal data breach.
- Upon discovery of a personal data breach or suspected personal data breach inform their line manager and Longford County Council's Data Protection & Information Compliance Officer and complete the Council's internal Data Breach Report (Appendix 1).

Data Protection & Information Compliance Officer

- Maintain the Council's Personal Data Breach Register detailing all reportable and non-reportable personal data breach incidents which occur within the organisation.
- Provide data protection advice and information to employees & line managers in the event of a personal data breach.
- Report a personal data breach to the Supervisory Authority
- Report a personal data breach to the affected Data Subject(s) where required
- Update Management Team as required
- On receipt of notification of a personal data breach carry out a risk assessment immediately or within a prescribed period not later than 72 hours
- Monitor implementation & review of this Policy
- Review the Council's Personal Data Breach Register and recommend appropriate revisions to policy and corrective actions and additional security measures for implementation as necessary.
- In the case of a personal data breach where Longford County Council are the Data Processor, the Council's Data Protection & Information Compliance Officer shall notify the Data Controller as soon the Council become aware of the data breach
- Assist with Data Protection training for all employees as required.

Human Resources

- Make available a copy of the policy to all new employees and provide induction training on policy requirements as part of the induction process
- In conjunction with the Corporate Services section, schedule and provide Data Protection training for all employees
- Obtain signed confirmation that employees understand and will comply with the policy provisions

Confidentiality

Longford County Council take appropriate measures to store and process personal data (physical and electronic) in a confidential and secure manner. Personal data shall not be shared with any person who does not require access to the personal data. Where possible and appropriate, personal data processed, transmitted or stored on Council's operating systems shall be password protected and/or encrypted.

Data Protection

Longford County Council is committed to the privacy rights of individuals and respecting the rights of those whose personal data we collect and process in accordance with applicable law.

Internal Review

Employees have the right to request an internal review of actions and measures taken to implement this policy in relation to personal data breaches within their work area and can make their request to the Senior Executive Officer Corporate Services.

Policy Review

This policy will be subject to review one year from its implementation date or earlier if required.

Further Information

For further information on this Policy please contact the Council's Data Protection & Information Compliance Officer

dpo@longfordcoco.ie

Approved by: _____

Date: _____

