National Parents Council Primary Data Protection Policy

Table of Contents

National Parents Council Primary Data Protection Policy

Introduction:

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of National Parents Council Primary. This includes obligations in dealing with personal and sensitive personal data (see Appendix 1), in order to ensure that the organisation complies with the requirements of the relevant Irish Data Protection legislation. This policy was formulated in May 2018, updating existing NPC data protection.

Rationale:

National Parents Council Primary must comply with the Data Protection principles set out in the relevant legislation. This Policy applies to all Personal and Sensitive Personal Data collected, processed and stored by National Parents Council Primary in relation to its staff, service providers and members in the course of its activities. National Parents Council Primary makes no distinction between the rights of Data Subjects who are employees, and those who are not. All are treated equally under this Policy.

Scope:

The policy covers both personal and sensitive personal data held in relation to data subjects by National Parents Council Primary. The policy applies equally to personal data held in manual and electronic form.

All Personal and Sensitive Personal Data will be treated with equal care by National Parents Council Primary. Both categories will be equally referred to as Personal Data in this policy, unless specifically stated otherwise.

This policy should be read in conjunction with the associated Data Subject Access Request procedure, the Data Retention and Destruction procedure and the Personal Data Security Breach procedure (see Appendices 2, 3 & 4)

National Parents Council Primary as a Data Controller

In the course of its daily organisational activities, National Parents Council Primary acquires, processes and stores personal data in relation to:

- Employees of National Parents Council Primary
- Members of National Parents Council Primary
- Special Interest Group members of National Parents Council Primary
- Trustees of National Parents Council Primary
- Volunteers of National Parents Council Primary
- Contacts/Mailing list of National Parents Council Primary
- Action Teams for Partnerships coordinated by National Parents Council Primary
- Interviewees and applicants to National Parents Council Primary
- Contracted trainers engaged by National Parents Council Primary

- Customers of National Parents Council Primary
- Third party service providers and suppliers engaged by National Parents Council Primary.

In accordance with the Irish Data Protection legislation, this data must be acquired and managed fairly. Not all staff members will be expected to be experts in Data Protection legislation. However, National Parents Council Primary is committed to ensuring that its staff have sufficient awareness of the legislation in order to be able to anticipate and identify a Data Protection issue, should one arise. In such circumstances, staff must ensure that the staff member with responsibility for Data Protection is informed, in order that appropriate corrective action is taken.

The Data Protection Principles:

The following key principles are enshrined in the Irish and EU legislation, including GDPR and are fundamental to the National Parents Council Primary's Data Protection policy.

In its capacity as Data Controller, National Parents Council Primary ensures that all data shall:

1. *... be processed lawfully, fairly and in a transparent manner*

For data to be obtained in this manner, the data subject will, at the time the data are being collected, be made aware of:

- The identity of the Data Controller (National Parents Council Primary)
- The purpose(s) for which the data is being collected
- The person(s) to whom the data may be disclosed by the Data Controller
- Any other information that is necessary so that the processing may be fair.

National Parents Council Primary will meet this obligation in the following way:

- The informed consent of the Data Subject will be sought before their data is processed;
- Where it is not possible or necessary to seek consent, National Parents Council Primary will ensure that collection of the data is justified under one of the other lawful processing conditions – legal obligation, contractual necessity, etc.;
- Processing of the personal data will be carried out only as part of National Parents Council Primary's lawful activities, and National Parents Council Primary will safeguard the rights and freedoms of the Data Subject;
- The Data Subject's data will not be disclosed to a third party without prior consent from the Data Subject and on receipt of such consent only to a party contracted to National Parents Council Primary and operating on its behalf.

2. *.... be collected for specified, explicit and legitimate purposes.*

National Parents Council Primary will obtain data for purposes which are specific, lawful and clearly stated. A Data Subject will have the right to question the purpose(s) for which National

Parents Council Primary holds their data, and National Parents Council Primary will be able to clearly state that purpose or purposes.

National Parents Council Primary will meet this obligation in the following way:

- The informed granular consent of the Data Subject will be sought to contact them for specific reasons.
- Any use of the data by National Parents Council Primary will be compatible with the purposes for which the data was acquired.

3. *... be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)*

National Parents Council Primary will ensure that the data it processes in relation to Data Subjects are relevant to the purposes for which those data are collected. Data which are not relevant to such processing will not be acquired or maintained.

4. *... be kept accurate, complete and up-to-date where necessary.*

National Parents Council Primary will meet this obligation in the following way:

- Ensure that administrative and IT validation processes are in place to conduct regular assessments of data accuracy;
- Conduct periodic reviews and audits to ensure that relevant data is kept accurate and up-to-date. National Parents Council Primary conducts a review of sample data every six months to ensure accuracy; Staff contact details and details on next-of-kin are reviewed and updated every two years.
- Conduct regular assessments in order to establish the need to keep certain Personal Data.

5. *... be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data was processed (storage limitation).*

National Parents Council Primary has identified a number of data categories, with reference to the appropriate data retention period for each category. This applies to data in both a manual and automated format.

Once the respective retention period has elapsed, National Parents Council Primary undertakes to destroy, erase or otherwise put this data beyond use.

6. *... be processed in a manner that ensures appropriate security of the personal data*

National Parents Council Primary will employ high standards of security in order to protect the personal data under its care. Appropriate security measures will be taken to protect against unauthorised access to, or alteration, destruction or disclosure of any personal data held by National Parents Council Primary in its capacity as Data Controller.

Data Subject Access Request

National Parents Council Primary has implemented a Data Subject Access Request procedure (see Appendix 2) by which to manage data subject requests in an efficient and timely manner, within the timelines stipulated in the legislation.

Access to and management of data subject records is limited to those staff members who have appropriate authorisation and password access.

Where a formal request is submitted by a Data Subject in relation to the data held by National Parents Council Primary, such a request gives rise to access rights in favour of the Data Subject.

There are specific time-lines within which National Parents Council Primary must respond to the Data Subject, depending on the nature and extent of the request. Any formal, written request by a Data Subject for a copy of their personal data (a Subject Access Request) will be referred, as soon as possible, to the staff member with responsibility for Data Protection, and NPC will ensure that such requests are processed as quickly and efficiently as possible, but within not more than one month from receipt of the request.

It is intended that by complying with these guidelines, National Parents Council Primary will adhere to best practice regarding the applicable Data Protection legislation.

Implementation

As a Data Controller, National Parents Council Primary ensures that any entity which processes Personal Data on its behalf (a Data Processor) does so in a manner compliant with the Data Protection legislation.

NPC does not share personal data with third parties, however in the course of surveying our members and contacts NPC uses SurveyMonkey, as such any information entered by the data subject will be stored temporarily in the US and by taking part in these surveys the data subject is consenting to any information that can identify them as an individual being stored in this way. SurveyMonkey is EU-US Privacy Shield Certified, the Privacy Shield is a mechanism that was approved by the EU as an adequate means for transferring personal data from the EU to the U.S. As such, the Privacy Shield is compliant with EU privacy law under the current Privacy Directive 1995/46/EC and, unless and until the EU decides to reverse its adequacy finding decision, it will remain so under GDPR.

Failure of a Data Processor to manage National Parents Council Primary's data in a compliant manner will be viewed as a breach of contract and will be pursued through the courts.

Failure of National Parents Council Primary's staff to process Personal Data in compliance with this policy may result in disciplinary proceedings.

Registering with the Data Protection Commissioner (DPC)

NPC is exempt from registering with the Office of the Data Protection Commissioner under section 16 1(B) Data Protection Act 1988 and 2003.

16 -(1) In this section 'person to whom this section applies' means a data controller and a data processor (other than such (if any) categories of data controller and data processor as may be specified in regulations made by the Minister after consultation with the Commissioner) except in so far as -

(b) the data controller is a body that is not established or conducted for profit and is carrying out processing for the purposes of establishing or maintaining membership of or support for the body or providing or administering activities for individuals who are either members of the body or have regular contact with it.

Appendices

Appendix 1: Definitions

For the avoidance of doubt, and for consistency in terminology, the following definitions will apply within this Policy.

Data	This includes both automated and manual data. Automated data means data held on computer or stored with the intention that it is processed on computer. Manual data means data that is processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.
Personal Data	Information which relates to a living individual, who can be identified either directly from that data, or indirectly in conjunction with other data which is likely to come into the legitimate possession of the Data Controller.
Sensitive Personal Data	A particular category of Personal data, relating to: Racial or Ethnic Origin, Political Opinions, Religious, Ideological or Philosophical beliefs, Trade Union membership, Information relating to mental or physical health, information in relation to one's Sexual Orientation, information in relation to commission of a crime and information relating to conviction for a criminal offence.
Data Controller	A person or entity who, either alone or with others, controls the content and use of Personal Data by determining the purposes and means by which that Personal Data is processed, in this case NPC.
Data Subject	A living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.
Data Processor	A person or entity who processes Personal Data on behalf of a Data Controller on the basis of a formal, written contract, but who is not an employee of the Data Controller, processing such Data in the course of his/her employment.
Relevant Filing System	Any set of information in relation to living individuals which is not processed by means of equipment operating automatically (computers), and that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable.

Appendix 2: Data Subject Access Request Procedure

Data subjects have the right to obtain confirmation as to whether their personal data are being processed by NPC and if so access to the following information:

a) The purpose of the processing
b) The personal data being processed
c) To whom the personal data has been or will be shared
d) The length of time the personal data will be stored
e) The right to request personal data be rectified (if inaccurate) or deleted
f) The right to lodge a complaint with the Data Protection Commissioner
g) The right to know where NPC sourced their personal data if not provided by the data subject

Under GDPR, NPC must deal with Data Access Requests within **one month**; there is scope to increase this timeframe by a further two months where a request is particularly complex.
Also, under GDPR, NPC will process data access requests for free, however it will be possible to charge a "reasonable fee" to the data subject to cover administrative charges where the request involves the gathering of large amounts of data.
The data subject will be entitled to receive a copy of their personal data in printed or electronic format as per their own specific preference.

Appendix 3: Data Retention and Destruction Procedure

The Data Protection Acts and GDPR require that personal information is kept for no longer than is necessary, but it does not stipulate the retention periods for different types of data. It requires organisations to have a retention policy in place for the personal data it holds which can take account of any statutory retention periods to which the organisation is subject.

If the purpose for which personal data was obtained has ceased and the personal information is no longer required, NPC will delete or dispose of the personal data in a secure manner. It may also be anonymised to remove any personal data.

NPC's Retention Policy is available on request.

Appendix 4: Personal Data Security Breach procedure

If a personal data security breach occurs, NPC will, without delay and where feasible not later than 72 hours after becoming aware of the breach notify the Data Protection Commissioner unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject.
Any delay in notification to the DPC beyond the 72 hours will be accompanied by reasons for the delay.
NPC will document any personal data breaches, including all facts and measures taken.

The notification to the DPC will include:

a) a description of nature of the personal data breach, including the categories and approximate number of data subjects concerned
b) the name and contact details of the Data Controller's employee with responsibility for dealing with Data Protection where further information can be obtained
c) the likely consequences of the personal data breach
d) the measures taken or proposed measures to be taken to address the personal data breach

Where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject NPC will also notify the data subject without undue delay.

The notification to the data subject will include:

a) the nature of the personal data breach
b) the name and contact details of the Data Controller's employee with responsibility for dealing with Data Protection where further information can be obtained
c) the likely consequences of the personal data breach
d) the measures taken or proposed measures to be taken to address the personal data breach