



club gan ainm!

# The No Name! Club

## Data Protection Policy

Document Title	No Name! Club Data Protection Policy			
Developed by:	Policy Committee of No Name! Club			
Approved by:	Carole Goulding (Chairperson of No Name! Club).			
Person Responsible for	Policy Committee Chairperson			
Document No.	P008	No. of Pages: 6		
Documentation History	Approved Date	Reviewed Date	Effective Date	Date Withdrawn
P.008	28 June 2016		29 June 2016	
Next review date; on or before 28 June 2017 (or earlier in the event of legislative update)				



No Name! Club complies with the Data Protection Act 1988 and the 2003 Amendment Act that brought Irish law into line with the EU Data Protection Directive 95/46/EC. All Sections of the Acts are in force.

In the course of their work, No Name! Club is required to collect and use certain types of information about people, including 'personal data' as defined by the Data Protection Acts. This information can relate to Young people, volunteers, current, past and prospective employees, suppliers and others with whom staff communicate. In addition, staff may occasionally be required to collect and use certain types of personal information to comply with the requirements of legislation. No Name! Club creates, collects and processes data in multiple formats.

**No Name! Club has a responsibility to ensure that this data is;**

- obtained fairly
- recorded correctly, kept accurate and up-to-date
- used and shared both appropriately and legally
- stored securely
- not disclosed to unauthorised third parties
- disposed of appropriately when no longer required, that is for the life time of the volunteer or minimum three years, maximum seven years.

All staff working for No Name! Club are legally required under the Data Protection Acts 1988 and 2003 to ensure the security and confidentiality of all personal data they collect and process. Data Protection rights apply whether the personal data is held in electronic format or in a manual or paper based form. Staff breaches of data protection legislation may result in disciplinary action.

**Data in the possession of NNC is used by the Organisation for –**

- Staff Employment and Payroll purposes
- Company Membership and compliance with relevant legislation
- Club Youth Membership
- Membership of Board of Directors
- Club Officials including volunteers, trainers and others involved in development
- Compliance where required with Garda Vetting and Insurance cover.

**Data Controllers for No Name! Club:**

- **Executive Program Manager**
- **Data/ Financial Manager**
- **Designated Liaison Officer**
- **Chairperson of the Board of No Name! Club or their nominee**

## DEFINITIONS

As with any legislation, certain terms have particular meaning.

**Data:** means information in a form which can be processed. It includes both automated data and manual data.

**Automated data:** means, broadly speaking, any information on a computer, or information recorded with the intention of putting it on a computer.

**Manual data:** means information that is kept as part of a relevant filing system, or with the intention that it should form part of a relevant filing system.

**Relevant filing system:** means any set of information that, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information is accessible.

**Personal data:** means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller. This can be a very wide definition depending on the circumstances.

**Processing:** means performing any operation or set of operations on data, including:

- obtaining, recording or keeping data
- collecting, organising, storing, altering or adapting the data
- retrieving, consulting or using the data
- disclosing the information or data by transmitting, disseminating or otherwise making it available
- aligning, combining, blocking, erasing or destroying the data.

**Data Subject** is an individual who is the subject of personal data.

**Data Controllers** are those who, either alone or with others, control the contents and use of personal data. Data Controllers can be either legal entities such as companies, Government Departments or voluntary organisations.

**Data Processor** is a person who processes personal data on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of his/her employment.

**Sensitive personal data** relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.

## DATA PROTECTION – IT'S EVERYONE'S RESPONSIBILITY Protecting Data.

1. Staff should operate a clear desk policy at the end of each working day and when away from the desk or the office for long periods.
2. Personal information should not be deliberately or inadvertently viewed by uninvolved Parties.
3. Personal and sensitive records held on paper and/or on screens must be kept hidden from callers to offices.
4. Records containing personal information must never be left unattended where they are visible or maybe accessed by unauthorised staff or members of the public.
5. If computers or VDUs are left unattended, staff must ensure that no personal information may be observed or accessed by unauthorised staff or members of the public.
6. The use of secured screen savers is advised to reduce the chance of casual observation.
7. Rooms, cabinets or drawers in which personal records are stored should be locked when unattended. A record tracing system should be maintained of files removed and/or returned.
8. While appreciating the need for information to be accessible, staff must ensure that personal records are not left on desks or workstations at times when unauthorised access might take place.
9. Do not leave information/data unattended in cars.
10. Staff must not leave laptops/portable electronic devices and/or files containing personal information unattended in cars.
11. All files and portable equipment must be stored securely. If files containing personal information must be transported in a car, they should be locked securely in the boot for the minimum period necessary.
12. When using the postal system, mail containing sensitive personal information should be marked clearly with "Strictly Private and Confidential". If proof of delivery is necessary, information of this nature should be sent by registered post. Please also provide "return to sender" information in the event that the mail is undeliverable.

**13. Staff must adhere to the No Name! Club Password Standards Policy:**

- All passwords must be unique and must be a minimum of 8 characters.
  - Passwords must contain a combination of letters (both upper & lower case), numbers (0-9) and at least one special character (for example: “, £, \$, %, ^, &, \*, @, #, ?, !, €).
  - Passwords must not be left blank.
  - Users must ensure passwords assigned to them are kept confidential at all times and are not shared with others including co-workers or third parties.
  - In exceptional circumstances where a password has to be written down, the password must be stored in a secure locked place, which is not easily accessible to others.
  - Staff must ensure that minimum personal information is stored on Portable devices, it is the responsibility of each device owner to ensure that the device is appropriately secured.
14. Where possible all confidential and personal information must be stored on a secure Basis.
  15. No Name! Club computers used by employees to work from home (home working) must have password protection and have up to date anti-virus software installed.

16. Only No Name! Club approved USB memory sticks which are distributed by No Name! Club may be used to store or transfer No Name! Club data.
17. No Name! Club employees who have been issued with an approved USB memory stick must take all reasonable measures to ensure the memory stick is kept secure at all times and is protected against unauthorised access, damage, loss and theft.

## **18. Mobile Phones**

- All Staff must ensure that no sensitive information relating to No Name! Club is stored on their mobile phone.

## **19. Organisations providing services on the No Name! Club behalf:**

- Where the No Name! Club engages a third party to provide services on its behalf and where the services require the service provider to process personal data, the No Name! Club is required by law to have a written contract in place with the service provider which provides sufficient guarantees with regard to data protection compliance.

## **20. Disposal of records**

- It is vital that the process of record disposal safeguards and maintains the confidentiality of the records. This can be achieved internally or via an approved records shredding contractor, but it is the responsibility of the service to satisfy itself that the methods used provide adequate safeguards against accidental loss or disclosure of the records.
- A register of records destroyed should be maintained as proof that the record no longer exist.

The register should show:

- - name of the file
- - former location of file
- - date of destruction
- -Who gave the authority to destroy the records?

## **What is Confidential?**

- Any records containing personal identifiable information such as name, address, date of birth, PPS Number, employee number, or medical record is deemed confidential.
- Other records may also be confidential if they contain information about No Name! Club business or finances. Examples of confidential documents include financial records, payroll records, personnel files, legal documents or medical records.

## **Segregation of confidential waste**

- Only a minority of documents are confidential, and should be disposed in confidential paper bins or security bags. Alternative paper recycling options should be provided for non-confidential paper/magazines.
- No Name! Club staff may shred confidential records into confetti-like particles using in-house shredders. This shredded paper can be recycled as part of a recyclables collection.

## **Data Protection Breaches**

- If personal data is inadvertently released to a third party without consent, this may constitute a breach of the Data Protection Acts. If a staff member is aware of a breach or suspected breach of the Data Protection Act they must; Implement the No Name! Club Breach Management Policy

## **No Name! Club Breach Management Policy**

A breach must be brought to the attention of the Data Controller who when informed of the breach will discuss with the Data Controllers the procedure to be followed including but not to the following:

- Identification and Classification - what information was breached and how sensitive is it?
- Containment and Recovery – minimise the damage and retrieve the data if possible.
- Risk Assessment – what are the potential adverse consequences of this breach?
- Notification of Breach – No Name! Club
- Evaluation and Response – aim to establish how the breach occurred and take action to ensure it doesn't occur again.
- Comply with requirements/recommendations of the Data Protection Commissioner's office.

**Please note; Data Protection Breaches have to be reported to the Data Protection Commissioner.**

## **Responsibilities of Data Controller**

### **Data Controllers for No Name! Club:**

- **Executive Programme Manager**
- **Data/ Financial Officer**
- **Designated Liaison Officer**
- **Chairperson of the Board of No Name! Club or their nominee**

Key responsibilities in relation to the Information /Data Processed and Held.

- You must make yourself aware of your data protection responsibilities, in particular, to process personal data fairly

- You should ensure that your staff and volunteers are made aware of their responsibilities through appropriate induction training with refresher training as necessary and the availability of an internal data protection policy that is relevant to the personal data held by you
- An internal policy which reflects the eight fundamental data protection rules and applies them to your organisation, which is enforced through supervision and regular review and audit
- A data controller found guilty of an offence under the Acts can be fined amounts up to €100,000, on conviction on indictment and/or may be ordered to delete all or part of the database
- Obtain and process information fairly
- Keep it only for one or more specified, explicit and lawful purposes
- Use and disclose it only in ways compatible with these purposes
- Keep it safe and secure
- Keep it accurate, complete and up-to-date
- Ensure that it is adequate, relevant and not excessive
- Retain it for no longer than is necessary for the purpose or purposes
- Give a copy of his/her personal data to an individual, on request.

### **Training & Education**

- All Staff and Volunteers must know about the levels of awareness of data protection in our organisation
- Staff and Volunteers must be aware of their data protection responsibilities - including the need for confidentiality

### **Co-ordination and Compliance**

- Data protection co-ordinator is the Secretary to the Board of No Name! Club and Data compliance person is the Chair of the No Name! Club Policy Committee
- All staff and Volunteers must be aware of Data protection co-ordinator and compliance person
- Formal review by the co-ordinator and compliance person of data protection activities within the organisation on an annual basis or as necessary
- Data Protection Policy

### **Procedures and Guidelines**

No Name! Club is firmly committed to ensuring personal privacy and compliance with the Data Protection Acts, including the provision of best practice guidelines and procedures in relation to all aspects of Data Protection.

- No Name! Club Data Protection Policy can be accessed on our Website [nonameclub.ie](http://nonameclub.ie)
- Access Requests Policy & Procedure can be located on our Website [nonameclub.ie](http://nonameclub.ie)
- Access Request Form

### **Review**

This Data Protection Policy will be reviewed regularly in light of any legislative or other relevant developments.



**No Name! Club**  
**Tel: 059 6400299**  
**e-mail: [info@nonameclub.ie](mailto:info@nonameclub.ie)**  
**website: [www.nonameclub.ie](http://www.nonameclub.ie)**

