INSERT CENTRE NAME
Centre Address

Web:
Email:

Data Protection Policy 2018

Introduction

At INSERT CENTRE NAME, privacy and data protection rights are very important to us.

All personal data will be maintained in accordance with the obligations of the **Data Protection Acts** and **The General Data Protection Regulation.**

Data Protection is the safeguarding of the privacy rights of individuals in relation to the processing of personal data, in both paper and electronic format. There are strict rules about the way in which personal data and sensitive personal data are collected, accessed, used and disclosed. Individuals are permitted to access their personal data on request, and confer on individuals the right to have their personal data amended if found to be incorrect.

Personal information means information that identifies you as an individual, such as:

- name
- postal address
- email address
- telephone number
- Personal information may also be a combination of data that combined can identify you

Sensitive personal information means information about:

- race or ethnic origin
- political opinions
- religious or similar beliefs
- trade union membership
- physical or mental health or condition or sexual life
- the commission of, or proceedings for, any offence committed or alleged to have been committed by you, the disposal of such proceedings or the sentence of any court in such proceedings

This document outlines INSERT CENTRE NAME's policy to help ensure that we comply with the Data Protection Acts.

The document is for all INSERT CENTRE NAME staff.

Purpose of this policy

This policy is a statement of INSERT CENTRE NAME's commitment to protect the rights and privacy of individuals in accordance with the Data Protection Acts.

It supports the GDPR Data Mapping document which describes specific data processes in detail and their relationship to current data rules.

Collecting information

INSERT CENTRE NAME recognizes the need to hold personal data about individuals for the following purposes:
THESE ARE RCNI EXAMPLES – PERSONALISE THIS SECTION TO YOUR OWN CENTRE

- Provision of the Garda Vetting service for Rape Crisis Centres
- Maintenance of the Register of RCNI Counsellors
- Registration for training programmes provided or organised by the INSERT CENTRE NAME
- Confidential engagement with individual clients such as Legal Policy Director client activity
- Complaints processing
- Payment of expenses to individuals
- Fulfilment of grant funding report requests (data is anonymised for reporting)
- Delivery and maintenance of the INSERT CENTRE NAME Database
- To perform accounting and other record-keeping functions.
- To provide personnel, payroll and pension administration services

Data Process Mapping

We will map and record all our personal data processing. We will keep these mappings under review and update them as relevant. We will ensure all members of staff and volunteers understand their individual and shared responsibility to INSERT CENTRE NAME's data protection role as Controller and Processer. We have a designated Data Compliance Officer (DCO) who is responsible for the data protection policy.

INSERT CENTRE NAME Data Compliance Officer is …. (RCNI's is Cliona – Note: *not necessarily* your data Collection Officer)

Privacy Impact Assessment

When commencing a new data collection programme or a project that involves personal data we will conduct a privacy impact assessment. We will involve a range of relevant stakeholders to the proposed project in that assessment including the potential data subjects. We will seek the support of external expertise through Rape Crisis Network Ireland or other experts to inform our assessment.

Data Protection Principles

We shall perform our data protection responsibilities in accordance with the following eight Data Protection principles:

1. **Obtain and process information fairly**

- We shall obtain and process personal data fairly and in accordance with statutory and other legal obligations.

- Our data collection aims to be open and transparent at all times. At the time we collect information about individuals, they are made aware of how that information will be used.

- For all requests for disclosure of personal data to third parties, consent is always sought in advance of any such disclosure, with very few exceptions relating to the reporting of child protection concerns and rare emergencies which do not allow enough time for consent to be sought

- If it is not implicit, special attention will be drawn to that fact, and consent obtained for any use beyond the primary expressed or implied reason.

2. **Keep it only for one or more specified, explicit and lawful purposes**

- We shall keep personal data for purposes that are specific, lawful and clearly stated.

- Personal data will only be processed in a manner compatible with these purposes.

- If the scope of use has potential to be increased, the individual will be contacted and consent obtained for each new specific purpose prior to any activity.

3. **Use and Disclosure**

- We shall use and disclose personal data only in circumstances that are necessary for the purposes for which we collected the data.

- Individuals are made aware of all requests for disclosure to third parties, and consent is sought for such disclosures unless falling under a legal basis beyond consent e.g. to protect vital interests such as mandatory reporting of child protection concerns

- Disclosures are typically related to the further provision of service to an individual and consent for this is explicitly sought using the application form.

- If disclosure of personal data to a third party is required which exceeds the terms of the provision within the consent declaration on the application form, consent will always be sought in such cases.

- Letters to external agencies containing personal data about an individual (e.g. letters of referral) form part of an individual's record and are maintained as part of the person's record.

- There are special circumstances under which disclosure of personal data to third parties without consent is allowed. These are provided for under the Data Protection legislation and are:

    - As ordered by the Gardai, or army personnel
    - For the purpose of investigating an offence
    - To protect the state's international relations
    - To prevent urgent injury or damage to person or property
    - Under a court order or other rule of law
    - Required for the purposes of obtaining legal advice or for legal proceedings in which the person making the disclosure is a party or a witness
    - Made at the request of and with the consent of the subject of the data

  In all such cases, full reference will be made to the current legislation

4. Keep it safe and secure

- We shall take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of personal data and against its accidental loss or destruction.

- All personal data is maintained in a secure manner. The following physical and software safeguards are in place to protect personal data:
  THESE ARE RCNI EXAMPLES – PERSONALISE THIS SECTION TO YOUR OWN CENTRE
    - Paper files containing sensitive personal data are maintained securely in locked cabinets within the RCNI office which is secured when unoccupied by RCNI staff
    - Paper files containing non-sensitive personal data are stored in the office which is secured when unoccupied by RCNI staff
    - Electronic records are maintained securely on a cloud based system with secure passwords to access both the computer device and cloud based system
    - No data is stored on a laptop hard drive retained for use by any RCNI staff member
    - The RCNI office is located within a locked external building

5. Keep it accurate, complete and up-to-date

- We adopt procedures that ensure high levels of data accuracy, completeness and that data is up-to-date.

6. **Ensure it is adequate, relevant and not excessive**

- We shall only hold personal data to the extent that it is adequate, relevant and not excessive.

- We collect and maintain sufficient information for the declared purpose in order to provide a fair and comprehensive service to each person.

- We only hold that information which is adequate and relevant to the purpose it serves.

7. **Retain for no longer than is necessary**

- Personal information processed/kept for any purpose should not be kept longer than is necessary for that purpose.

- The minimum period set down for the retention of records is seven years generally. However, any destruction of material must be considered carefully if it is to be carried out before the minimum time period. Any such actions would need to be justified to the Board.

- Purging of data occurs on an annual basis, and as once-offs on completion of purpose.

- All records will be destroyed in accordance with Data Protection law.

- All records will be destroyed in a manner that eliminates the possibility of reconstruction of the information. Paper records will be destroyed by shredding. Any CD-RW disks that contain document imaging that cannot be overwritten will be destroyed through pulverization.

- All records involved in any investigation, litigation, or audit will not be destroyed until it has been confirmed that no further legal reason exists for retention of the record.

8. **Give a copy of his/her personal data to that individual, on request**

- All individuals have the right to access all the personal data held on them by INSERT CENTRE NAME.

- Personal data will normally be accessible using the **Personal Data Access Procedure**. (See Attachment 1)

- INSERT CENTRE NAME takes the stance that individuals may need assistance to request access to their own personal data. INSERT CENTRE NAME will provide advice on the easiest route to achieve this.

Procedures and Guidelines

INSERT CENTRE NAME 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.

This policy is circulated to all new staff as part of their induction process.

Signed: Signed:

Chairperson Executive Director [edit if applicable]

Date: Date:

Personal Data Access Procedure

- All requests must be made in writing with the consent of the person served
- All requests should be made using the form attached and sent to:
    - Executive Director [edit if applicable]
      INSERT CENTRE NAME
      Insert Address
- Proof of identity and address of the person served should accompany the Personal Data Request Form
- Where requests are received in writing not using the standard form, e.g. from solicitors, the validity of the request must be checked. The request must quote the Data Protection legislation and also include the person served written consent. When in doubt, revert to the requestor with the standard form.
- The Executive Director [edit if applicable] must be notified of all requests for disclosure of personal information.
- The Executive Director [edit if applicable] will record the request and coordinate the file duplication and disclosure process.
- The information will be supplied within 30 days.
- For requests to access the RCNI Database, please refer to the RCNI Database Access Protocol

Attachment 1

Personal Data Request Form

Executive Director [edit if applicable]
INSERT CENTRE NAME
Insert address

[Date]

Dear Sir/Madam,

I wish to make an access request under the Data Protection Acts 1988 and 2003 for a copy of any information you keep about me, on computer or in manual form. I am making this request under section 4 of the Data Protection Acts.

Regards

[signed]

[your name]

NAME (please print) _____

ADDRESS:_____
_____
_____

Please Note:

1. Request in writing should be made and signed by the applicant in person.
2. Within the terms of the Data Protection Act 1988/2003, INSERT CENTRE NAME will respond to your request for personal data within 30 days.
3. Attach a photocopy of your proof of identity and address to the Personal Data Request Form
4. Requests should be submitted to: Executive Director [edit if applicable], INSERT CENTRE NAME, Insert address

Procedure for Data Loss Notification

- A breach is a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, for an authorized purpose, have access or potential access to personal data in usable form, whether manual or automated.

  This could mean:

  - Loss of a laptop, memory stick or mobile device that contains personal data
  - Lack of a secure password on PCs and applications
  - Emailing a list to someone in error
  - Giving a system login to an unauthorised person
  - Failure of a door lock or some other weakness in physical security which compromises personal data

- Actual, suspected, or potential breaches should be reported immediately to the INSERT CENTRE NAME Executive Director [edit if applicable] who will assess the breach and determine its severity, and coordinate the appropriate course of action.

- Any employee who becomes aware of a likely data breach and fails to notify the Executive Director [edit if applicable] could be subject to INSERT CENTRE NAME's disciplinary procedure.

- All data breaches will be recorded in an **incident log** as required by the Office of the Data Protection Commissioner.