Data Protection Policy

Table of Contents

Introductory Statement

Data Protection Policy of Connect RP

CONNECT RP's Data Protection Policy applies to the personal data held by us which is protected by the Data Protection Acts 1988 and 2003 now superseded by the GDPR 2016/679 (General Data Protection Regulation 2016/679). The policy applies to all information held and processed (including prospective or potential participants/ clients and their organisations) insofar as the measures under the policy relate to them. Data will be stored securely, so that information is protected in compliance with relevant legislation. This policy sets out the way in which personal /school – organisation data will be protected by CONNECT RP.

Data Protection Principles

CONECT RP is the ***data controller*** of ***personal data*** relating to its past, present and future clients/participants. CONNECT RP is obliged to comply with the principles of data protection set out in the Data Protection Acts 1988 and 2003 which can be summarised as follows:

- **Obtain and process** *Personal Data* **fairly**: Information on CONNECT RP customers/ participants/ is gathered directly from participants themselves or via their associated organisations/ schools. All such data is treated in accordance with the Data Protection Acts and the terms of this Data Protection Policy. The information will be obtained and processed fairly. This will be achieved by adopting appropriate data protection notices at the point of data capture e.g. on our website where consent is requested or at any of our course days where forms specify that all information collected will be processed and managed under the guidelines of GDPR. The inclusion of information on these forms is taken as the individual consenting to their data being used by CONNECT RP for the purposes specified on the form.
- The information is generally furnished by the individuals themselves with full and informed consent and used during the course of their engagement with CONNECT RP.
- **Keep it only for one or more specified and explicit lawful purposes**: CONECT RP will inform individuals of the reasons they collect their data and will inform individuals of the uses to which their data will be put. All information is kept with the best interest of the individual in mind at all times.
- **Process it only in ways compatible with the purposes for which it was given initially**: Data relating to individuals will only be processed in a manner consistent with the purposes for which it was gathered. Information will only be disclosed on a need to know basis, and access to it will be strictly controlled. Data may be disclosed to third parties including: An Garda Síochána, Data Commissioners. It may also be necessary to disclose information in order to comply with any legal obligations. CONECT RP takes all reasonable steps as required by law to ensure the safety, privacy and integrity of the information and, where appropriate, enter into contracts with such third parties to protect the privacy and integrity of any information supplied. CONECT RP will endeavour to comply with Data Commissioner Guidelines (https://www.dataprotection.ie/documents/guidance/GuidanceFinance.pdf) in relation to the transfer of data to third parties.

- **Keep** *Personal Data* **safe and secure**: Only those with a genuine reason for doing so may gain access to the information held by CONNECT RP. **CONNECT RP does not collect any sensitive personal data in its work**. Sensitive Personal Data (*defn. – page 4*)

- CONNECT RP stores personal information (in relation to participants/ schools/ organisations) in controlled access, centralised databases (including computerised and manual files) in its main office: 134 Carrigmore Crescent, Block 4, Citywest, D24, Ireland.
- CONNECT RP will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against its accidental loss or destruction. CONNECT RP acknowledges that high standards of security are essential for processing all personal information and endeavours to comply with the **Data Commissioner Guidelines** which contains comprehensive guidelines regarding best practice in the area of data security. Some of the security measures we take include:

- ❖ Access to files containing personal data (computerised and manual) is restricted to CONNECT RP staff.
- ❖ Computer systems are password protected and are backed up on an iCloud.
- ❖ Waste paper which may include school/organisation/ participant information is shredded

- **Keep Personal Data accurate, complete and up-to-date**: Participants/Schools/ Organisations, should inform CONNECT RP of any change which we should make to their personal data to ensure that the individual's data is accurate, complete and up-to-date. Once informed, we will make all necessary changes to our records. CONNECT RP may delegate such updates/amendments to any member of the admin staff. However, records must not be altered or destroyed without proper authorisation. If alteration/correction is required, then a note of the fact of such authorisation and the alteration(s) to be made to any original record/documentation should be dated and signed by the person making that change
- **Ensure that it is adequate, relevant and not excessive**: Only the necessary amount of information required to provide an adequate service will be gathered and stored. Personal data held by CONNECT RP will be adequate, relevant and not excessive in relation to the purpose/s for which it is kept. Periodic checks will be made of files (electronic and manual) to ensure that personal data held is not excessive and remains adequate and relevant for the purpose for which it is kept.
- **Retain it no longer than is necessary for the specified purpose or purposes for which it was given**: As a general rule, the information will be kept for the duration of the participants engagement with CONNECT RP and for 2 years thereafter. It will then be recorded and filed for 7 years.

In setting retention periods for different sets of data, regard will be taken of the relevant legislative and taxation requirements, the possibility of litigation, the requirement to keep an archive for historical purposes and the retention periods laid down by funding agencies e.g. European Structural Funds, NDP. Retention times cannot be rigidly prescribed to cover every possible situation and CONNECT RP will use the "Record Retention Schedule" of the Data Commissioner as a guideline only (https://www.revenue.ie/en/corporate/documents/records-retention-schedule.pdf. CONNECT RP reserves the right to exercise its judgment and discretion in relation to specific classes of data, taking account of its statutory obligations and best practice in relation to each category of records held.

- **Provide a copy of their** *personal data* **to any individual, on request**: Individuals have a right to know what personal data is held about them, by whom, and the purpose for which it is held.
  - ❖ On making an access request any individual about whom CONNECT RP keeps Personal Data, is entitled to a copy of their personal data and a description of:
  - ❖ The categories of data being processed,
  - ❖ The personal data constituting the data of which that person is the subject,
  - ❖ The purpose for the processing,
  - ❖ The recipients/categories of recipients to whom the data is or may be disclosed
  - ❖ Any information known or available to CONNECT RP as to the source of those data unless the communication of that information is contrary to the public interest

  To make an access request, the individual should read the CONNECT RP's "**Data Access Procedures" set out at the end of this document** and then complete the "Data Access Request Form" **set out at the end of this document.**

CONNECT RP

Scope

Purpose of the Policy: The Data Protection Acts 1988 and 2003 apply to the keeping and processing of *Personal Data*, both in manual and electronic form. The purpose of this policy is to assist us to meet our statutory obligations, to explain those obligations and outline how data will be treated.

The policy applies to all CONNECT RP staff, participants and clients -schools/organisations (including prospective or potential connections) insofar as CONNECT RP handles or processes their *Personal Data* in the course of their dealings with them.

Definition of Data Protection Terms

In order to properly understand our obligations, there are some key terms which should be understood by all reading this document:

Data means information in a form that can be processed. It includes both *automated data* (e.g. electronic data) and *manual data*. *Automated data* means any information on computer, or information recorded with the intention that it be *processed* by computer. *Manual data* means information that is kept/recorded as part of a *relevant filing system* or with the intention that it form part of a relevant filing system.

Data Controller for the purposes of this Policy is CONNECT RP.

Data Processor- in CONNECT RP's context this is an organisation contracted to process data on behalf of our company. In this context it may include cloud based administrative software such as intercom or teachable or the CONNECT RP website.

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 relating to a particular individual is readily, quickly and easily accessible. Examples might include school/organisation files stored in alphabetic order in a filing cabinet or participant files stored in the office.

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.

Sensitive Personal Data refers to *Personal Data* regarding a person's

- racial or ethnic origin, political opinions or religious or philosophical beliefs
- membership of a trade union
- physical or mental health or condition or sexual life
- commission or alleged commission of any offence or
- any proceedings for an offence committed or alleged to have been committed by the person, the disposal of such proceedings or the sentence of any court in such proceedings, criminal convictions or the alleged commission of an offence.

*** CONNECT RP WILL NEVER COLLECT SENSITIVE PERSONAL DATA IN ITS WORK*

Rationale

In addition to its legal obligations under the broad remit of educational legislation, CONNECT RP has a legal responsibility to comply with the Data Protection Acts, 1988 and 2003.

This policy explains what sort of data is collected, why it is collected, for how long it will be stored and with

whom it will be shared. As more and more data is generated electronically and as technological advances enable the easy distribution and retention of this data, the challenge of meeting our legal responsibilities has increased.

CONNECT RP takes its responsibilities under data protection law very seriously and wishes to put in place safe practices to safeguard individual's personal data. It is also recognised that recording factual information accurately and storing it safely facilitates an evaluation of the information, enabling CONNECT RP to make decisions in respect of the efficient running of the company. The efficient handling of data is also essential to ensure that there is consistency and continuity where there are changes of staff within CONNECT RP.

Personal Data

The *Personal Data* records held by CONNECT RP **may** include:

School/ Organisation records- point of contact:

As well as existing customers (Schools and organisations) & former customers, these records may also relate to organisations / schools looking to engage with the services and supports of CONNECT RP in the future.
These records may include:

- Name, address and contact details for the customer
- Name, address, email and phone number of a designated contact person
- Details of request – CPD/ Student based workshop / mediation agreements/
- Records of any previous work carried out with that organisation, for example post consultancy staff plans

Purposes:

School/ Organisation records are kept for the purposes of:

- Facilitating the management and administration of the work of CONNECT RP (now and in the future)
- To facilitate CONNECT RP in collecting payment for services delivered, and calculation of other benefits/ entitlements (mileage/ expenses/ resources)
- To enable the school to comply with its obligations as an employer including the preservation of a safe, efficient working and teaching environment (including complying with its responsibilities under the Safety, Health and Welfare At Work Act. 2005)

Location: Manual Records will be held in a secure, locked filing cabinet that only personnel who are authorised to use the data can access. CONNECT RP admin staff are required to maintain the confidentiality of any data to which they have access.

Security: Paper Records are kept in a secure filing cabinet in a locked filing cabinet in CONNECT RP's Main Office.

Computer records are kept on password protected PCs and cloud-based storage (Office 365/ google drive/ gmail) is protected by up to date security and enhanced data protection and controlled password protected access to information, relevant to each school/organisation. Office 365/ google drive/ Gmail, are password protected. CONNECT RP take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. CONNECT RP acknowledges that high standards of security are essential at a local level for processing all personal information.

Individual participant records:

Categories of data: These **may** include:

When you enter into a contract/agreement/ e-learning course with us (or someone does so on your behalf) there will be personal information about you collected relating to that contract.

We need this information to carry out our work with you and to support you and your organisation. You must therefore provide this in order to enter into a contract with us (or as required under that contract). This information generally includes:

- Your name.
- Your email * *we will always request and encourage the provision of work emails*
- Your school/organisation address
- Your school/organisation information including your principal/manager details if relevant.
- Name and contact details of individual consumers of our products or services covered by the contract.
- Other correspondence or interaction (for example by email, telephone, post, SMS or via our website) between you and us, will include personal information (such as names and contact details) in that correspondence. This may include enquiries, reviews, follow-up comments or complaints lodged by or against you.
- We may also collect details of phone numbers used to call our organisation and the date, time and duration of any calls.

Purposes: The purposes for keeping these records are:

- to comply with legislative or administrative requirements and ensure we meet our contractual obligations, to you
- to look after, manage and maintain your details when you book training;
- to fulfil and arrange delivery of orders/ courses/ resources you make using CONNECT RP;
- provide customer services to you, or the person you are purchasing on behalf of;
- communicate with you in respect of booking training or purchases or other enquiries you may make; and process payments from you, including card payments on the Eventbrite/ Stripe system/PO & Invoices

Purposes:

School/ Organisation records are kept for the purposes of:

- Facilitating the management and administration of the work of CONNECT RP (now and in the future)
- To facilitate CONNECT RP in collecting payment for services delivered, and calculation of other benefits/ entitlements (mileage/ expenses/ resources)
- To enable the school to comply with its obligations as an employer including the preservation of a safe, efficient working and teaching environment (including complying with its responsibilities under the Safety, Health and Welfare At Work Act. 2005)

Location: Manual Records will be held in a secure, locked filing cabinet that only personnel who are authorised to use the data can access. CONNECT RP admin staff are required to maintain the confidentiality of any data to which they have access.

Security: Paper Records are kept in a secure filing cabinet in a locked filing cabinet in CONNECT RP's Main Office. Computer records are kept on password protected PCs and cloud-based storage (Office 365/ google drive/ Gmail) is protected by up to date security and enhanced data protection and controlled password protected access to information, relevant to each school/organisation. Office 365/ google drive/ Gmail are password protected. CONNECT RP take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. CONNECT RP acknowledges that high standards of security are essential at a local level for processing all personal information.

Other online services used to store data include

- Teachable- records courses participants enrol in and their individual progress for certification purposes,

- Intercom platform used to record a list of participant names – past/ current / potential, email addresses/ correspondence.

- Online payment system – Eventbrite/ Stripe (note participant name, , email, date of purchase, credit card details – must be collected to activate an online course or attendance on a Saturday workshop.)

Other records:

CONNECT RP may hold other records relating to organisations/ individuals. The format in which these records will be kept are manual record (personal file within a relevant filing system), and/or computer record (database).

Creditors

Categories of data: CONNECT RP may hold some or all of the following information about creditors (some of whom are self-employed individuals):

- name
- address
- contact details
- PPS number
- Tax certs
- Bank details and
- Amount paid/ to be collected.
- Records of Transactions

Purposes: This information is required for routine management and administration of CONNECT RP's financial affairs, including the payment of invoices, the compiling of annual financial accounts and complying with audits and investigations by the Revenue Commissioners.

Location: In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

Security: Paper Records are kept in a secure filing cabinet in the main office.

Automated data is stored on a password protected laptop which then accesses password protected bank accounts. This aspect of CONNECT RP's operation is password protected. CONNECT RP take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction.

Links to other policies

CONNECT RP's policies need to be consistent with one another, within the framework of business plan. Relevant policies already in place or being developed or reviewed, shall be examined with reference to the data protection policy and any implications which it has for them shall be addressed.

The following policies may be among those considered:

- Cookie Policy
- Website Privacy Statement

Processing in line with data subject's rights

Data collected by CONNECT RP will be processed in line with the data subjects' rights.

Data subjects have a right to:

(a) Request access to any data held about them by a data controller

(b) Prevent the processing of their data for direct-marketing purposes

(c) Ask to have inaccurate data amended/ deleted

(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

Dealing with a Data Access Requests

1. ***Section 3 Access request- See more detail at the end of this document – page 10***

Under Section 3 of the Data Protection Acts, an individual has the right to be informed whether an organisation holds data/information about them and to be given a description of the data together with details of the purposes for which their data is being kept. The individual must make this request in writing and the data controller will accede to the request within 21 days.

The right under Section 3 must be distinguished from the much broader right contained in Section 4, where individuals are entitled to a copy of their data.

2. ***Section 4 access request – See Page 13***

Individuals are entitled to a copy of their personal data on written request.
The individual is entitled to a copy of their personal data (subject to some exemptions and prohibitions set down in Section 5 of the Data Protection Act)

- Request must be responded to within 20 days
- Fee may apply but cannot exceed €6.35

Where a subsequent or similar request is made soon after a request has just been dealt with, it is at the discretion of CONNECT RP as data controller to comply with the second request (no time limit but reasonable interval from the date of compliance with the last access request.) This will be determined on a case-by-case basis.

No personal data can be supplied relating to another individual unless that third party has consented to the disclosure of their data to the applicant. Data will be carefully redacted to omit references to any other individual and only where it has not been possible to redact the data to ensure that the third party is not identifiable would the school refuse to furnish the data to the applicant.

Providing information over the phone

Within CONNECT RP when dealing with telephone enquiries we will be careful about disclosing any personal information held by CONNECT RP over the phone. In particular we will:

- Check the identity of the caller to ensure that information is only given to a person who is entitled to that information
- Suggest that the caller put their request in writing if we are unsure about the identity of the caller and in circumstances where the identity of the caller cannot be verified
- No employee of CONNECT RP should feel forced into disclosing personal information past or present over the phone.

Implementation arrangements, roles and responsibilities

CONNECT RP is the data controller and Michelle Stowe (Director) will be assigned the role of co-ordinating implementation of this Data Protection Policy and for ensuring that staff who handle or have access to *Personal Data* are familiar with their data protection responsibilities.

The following personnel have responsibility for implementing the Data Protection Policy:

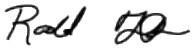
Name	**Responsibility**
CONNECT RP	Data Controller
Director of CONNECT RP:	Implementation of Policy
Admin Personnel	Awareness of responsibilities, Security, confidentiality
IT support	Security, encryption, confidentiality, password reminders

Ratification & communication

When the Data Protection Policy has been ratified by the Director of CONNECT RP, it becomes the agreed Data Protection Policy of CONNECT RP.

This Policy was adopted by CONNECT RP on
Date 20th Jan 2020

Signed Director 

Witness 

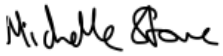
It is/will be published on the CONNECT RP website where it can be accessed.

Monitoring the implementation of the policy

The implementation of the policy shall be monitored by the Director of CONNECT RP.

Reviewing and evaluating the policy

The policy should be reviewed and evaluated at certain pre-determined times and as necessary. On-going review and evaluation should take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, Revenue Commissioner), legislation and feedback from participants and organisations who engage with the services of CONNECT RP.

Signed: 

For and behalf of CONNECT RP

Date: 20/01/2021

Data Access Procedures Policy

Date of adoption by CONNECT RP : Jan 2020

The Data Protection Acts, 1988 and 2003 provide for a right of access by an individual data subject to personal information held by *CONNECT RP*. The following procedure is provided to ensure compliance with our obligations under the Acts and governs the manner in which requests for access to personal data will be managed CONNECT RP . A data subject is required to familiarise themselves with the procedure and to complete the **Data Access Request Form** (see Appendix 2 of the Data Protection Policy) which will assist us in processing the access request where personal information as a data subject is processed and retained by *CONNECT RP.* It is important to note that only personal information relating to the individual will be supplied. No information will be supplied that relates to another individual.

Individuals making an access request

On making an access request, any individual about whom *CONNECRP* keeps *Personal Data* is entitled to:

- a copy of the data which is kept about him/her (unless one of the exemptions or prohibitions under the Data Protection Acts apply, in which case the individual will be notified of this and informed of their right to make a complaint to the Data Protection Commissioner)
- know the purpose/s for processing his/her data
- know the identity (or the categories) of those to whom the data is disclosed
- know the source of the data, unless it is contrary to public interest

Data access requirements

To make an access request, you as a data subject must:

Apply in writing requesting access to your data under section 4 Data Protection Acts or, alternatively, request an Access Request Form (see Appendix 2 of the Data Protection Policy) which will greatly assist us in processing your access request more quickly.

Correspondence should be addressed to CONNECT RP, 134 Carrigmore Crescent, Block 4, Citywest, D24, Ireland.

1. CONNECT RP reserves the **right to request official proof of identity** (e.g. photographic identification such as a passport or driver's licence) where there is any doubt on the issue of identification.
2. On receipt of the access request form, a member of the CONNECT RP team will check the validity of your access request and to check that sufficient information to locate the data requested has been supplied. It may be necessary to contact you in the event that further details are required with a view to processing your access request.
3. The CONNECT RP team member will log the date of receipt of the valid request and keep a note of all steps taken to locate and collate the requested data.
4. The CONNECT RP team member will ensure that all relevant manual files (held within a "relevant filing system") and computers are checked for the data in respect of which the access request is made.
5. The CONNECT RP team member will ensure that the information is supplied promptly and within the advised timeframes in items 7, 8 and 9 as appropriate.

6. **Where a request is made under Section 3 of the Data Protection Acts,** the following information will be supplied: (i) what CONNECT RP holds by way of personal information about you and (ii) a **description** of the data together with details of the purposes for which his/her data is being kept will be provided. Actual copies of your personal files (or the personal files relating to the student) will not be supplied. No personal data can be supplied relating to another individual. A response to your request will be provided within 21 days of receipt of the access request form and no fee will apply.
7. **Where a request is made under Section 4 of the Data Protection Acts,** the following information will be supplied within **20 days and an administration fee of €6.35 will apply.** The individual is entitled to a copy of all personal data, i.e.
    - A copy of the data which is kept about him/her (unless one of the exemptions or prohibitions under the Data Protection Acts applies, in which case the individual will be notified of this and informed of their right to make a complaint to the Data Protection Commissioner)
    - Be advised of the purpose/s for processing his/her data
    - Be advised of the identity (or the categories) of those to whom the data is disclosed
    - Be advised of the source of the data, unless it is contrary to public interest
    - where the processing is by automated means (e.g. credit scoring in financial institutions where a computer program makes the "decision" as to whether a loan should be made to an individual based on his/her credit rating), know the logic involved in automated decisions.
8. Before supplying the information requested to you as data subject (or where the access request is made on behalf of a student aged under 18 years, information relating to the student), the CONNECT RP team member will check each item of data to establish:
    - If any of the exemptions or restrictions set out under the Data Protection Acts apply, which would result in that item of data not being released, or
9. If data relating to a third party is involved, it will not be disclosed without the consent of that third party or alternatively the data will be anonymised in order to conceal the identity of the third party. Where it is not possible to anonymise the data to ensure that the third party is not identified, then that item of data may not be released.
10. Where CONNECT RP may be unsure as to what information to disclose, CONNECT RP reserves the right to seek legal advice.
11. The CONNECT RP team member will ensure that the information is provided in an intelligible form (e.g. codes explained) or will provide an explanation.
12. Number the documents supplied.
13. Have the response "signed-off" by an appropriate person, (Director of CONNECT RP).
14. CONNECT RP will respond to your access request within the advised timeframes contingent on the type of request made.
15. CONNECT RP reserves the right to supply personal information to an individual in an electronic format e.g. USB, CD etc.
16. Where a subsequent or similar access request is made after the first request has been complied with, CONNECT RP has discretion as to what constitutes a reasonable interval between access requests and this will be assessed on a case-by case basis.
17. Where you as an individual data subject may seek to rectify incorrect information maintained by CONNECT RP, please notify us and a form will be supplied to you for this purpose. You should however note that the right to rectify or delete personal data is not absolute. You have the right to make a complaint to the Data Protection Commissioner about a refusal.
18. In circumstances where your access request is refused, *CONNECT RP* will write to you explaining the reasons for the refusal and the administration fee, if provided, will be returned. In such circumstances, you have the right to make a complaint to the Office of the Data Protection Commissioner www.dataprotection.ie. Similarly, the administration access fee will be refunded to you if CONNECT RP has to rectify, supplement or erase your personal data.

Exceptions to note:
Data protection regulations **prohibit** the supply of:

The Data Protection Acts state that the following data is **exempt** from a data access request:

1. Section 5 of the Data Protection Act provides that the right of access does not apply in a number of cases in order to strike a balance between the rights of the individual, on the one hand, and some important needs of civil society on the other hand. Examples would include the need for state agencies (like An Garda Síochána) to **investigate crime** effectively and the need to protect the international relations of the State.
2. Section 4 states that the right of access does not include a right to see **personal data about another individual**, without that other person's consent. This is necessary to protect the privacy rights of the other person. If it is reasonable for CONNECT RP to conclude that redacting or omitting the particulars identifying the third party would both conceal the identity of the third party and enable the data to be disclosed (subject to the redactions), then the data could be disclosed with such redactions. However, if it is not possible to redact or omit the particulars which identify a third party, then the affected data should not be released to the applicant.
3. Section 4 also states that where personal data consists of **expressions of opinion** about the data subject made by another person, the data subject has a right to receive that expression of opinion **except** where that expression of opinion was given in confidence, and on the clear understanding that it would be treated as confidential.

Where CONNECT RP refuses to hand over some or all of the personal data they hold in relation to a data subject (on the basis of any of the exemptions or prohibitions set out above), CONNECT RP must advise the data subject of this in writing, setting out reasons for the refusal and notifying the data subject that he or she has the right to complain to the Office of the Data Protection Commissioner about the refusal.

Appendix
Data Access Request Form

Date:_____

Access Request Form: Request for a copy of Personal Data under the Data Protection Act 1988 and Data Protection (Amendment) Act 2003

Important: Proof of Identity must accompany this Access Request Form (eg. official/State photographic identity document such as driver's licence, passport).

A fee of €6.35 must accompany this Access Request Form if it is a Section 4 Data Access Request together with proof of identity (eg. official/State photographic identity document such as driver's licence, passport).

Full Name	
Address	
Contact number *	Email addresses *

** We may need to contact you to discuss your access request*

Please tick the box which applies to you:

Student ☐	Parent/Guardian of student ☐	Former Participant ☐
Current Participant ☐	Former Employee ☐	Other – Please specify

Section 3 Data Access Request:

I, …… [insert name] wish to be informed whether or not *CONNECT RP* holds personal data about me and to be provided with a description of this data and to be informed of the purpose for holding such data. I am making this access request under **Section 3** of the Data Protection Acts. ☐

OR

Section 4 Data Access Request:

I, …… [insert name] wish to make an access request for a copy of any personal data that *CONNECT RP* holds about me. I am making this access request under **Section 4** of the Data Protection Acts. ☐

Section 4 Data Access Request only: I enclose €6.35 ☐

Any other information relevant to your access request

Signed …… Date ……

Checklist: Have you:

1) Completed the Access Request Form in full? ☐
2) Included a cheque or postal order made payable to *CONNECT RP>* in the amount of €6.35 where a Section 4 request is made. (Please do not send us €6.35 if you are making a request under section 3. There is no administration charge for a section 3 request, and if you send us a cheque, it will be returned to you). ☐
3) Signed and dated the Access Request Form? ☐
4) Included a photocopy of official/State photographic identity document (driver's licence, passport etc.)*☐

- Please return this form to:
  CONNECT RP Data Protection Officer ,
  134 Carrigmore Crescent,
  Block 4,
  Citywest, D24, Ireland.

CONNECT RP - Records Management Procedures –

Note: This is an internal document. This does not have to be circulated with the policy

1. Purpose

Good records management is of special significance in the context of CONNECT RP's functions. We aim to implement records management procedures and to ensure preservation of records of permanent value and to establish archival criteria to maintain and assure continued access to appropriate historical records.

2. Ownership of Records

All records, irrespective of format, (i.e. both manual and automated data) created or received by CONNECT RP in the course of their services are the property of CONNECT RP and subject to its overall control. Any employees leaving CONNECT RP must leave all records intact for their successors and are not permitted to remove or retain records (in electronic or manual format) for any reason.

3. Management of CONNECT RP Records

- All records created and received CONNECT RP in the course of their services must be retained for as long as they are required to meet the legal, administrative, financial and operational requirements, after which time they are either destroyed or transferred to CONNECT RP archives.
- The final disposition (either destruction or transfer to the archives) of records is carried out according to approved Records Retention Schedules.
- While the Records Retention Schedule prescribes the minimum period that records must be retained, CONNECT RP may at their discretion, keep the records for a longer period of time if it is deemed necessary and appropriate, and where it is required for a specific purpose (e.g. the defence of litigation).
- A list of the vital records held within CONNECT RP, shall be reviewed periodically. For example, financial information, legal documentation etc. should be included in this.

4. Employee Duties

- All CONNECT RP employees are responsible for making and keeping the records of their work and shall: Comply with the "***Filing Guidelines" set out at Appendix A hereto"***.
- Create records needed to complete CONNECT RP business record decisions, actions taken, and generally document activities for which they are responsible. This means establishing or adhering to good directories and files, and filing materials (in any format) regularly and carefully in a manner that allows them to be safely stored and efficiently retrieved and returned when necessary.
- Ensure that all records under their control are stored/retained/destroyed or archived

5. Retention and Disposal

- After the records have been retained for the requisite time, they are either securely destroyed (e.g. by confidential cross-shredding or securely transferred to archival storage.
- It is the responsibility of the Director to ensure that records are scheduled as necessary to be retained in the appropriate storage facility or securely disposed of.

6. Life-Cycle of Records within CONNECT RP

- Each record has a Life Cycle, which is as follows:

Current Records	Are those that are held online/ in the office and are used on a very regular basis.
Non-current Records	These are records that are needed for occasional reference. Can be held on site in a dedicated storage area or stored online with easy access.
Disposition	Records which should either be archived or securely and confidentially cross-shredded.

Current Records:

- Active Records: Active records are records that are required and referred to constantly for current use, and which need to be retained and maintained in an area easily and readily accessible
- Semi-active Records: Semi-active records are records that are referred to infrequently and are not required constantly for current use. Semi-active records are removed from office space to storage until they are no longer needed.

Non-Current Records

- Inactive Records: Inactive records are records which are no longer required to carry out the functions for which they were created. They should be stored until the retention period has lapsed.
- Permanently Valuable Records – Archives: Permanently valuable records include those with legal, operational, administrative, historical, scientific, cultural and social significance.

APPENDIX A: Filing Guidelines

a) Before filing a piece of paper, ask yourself, "Will I need this in the future?" Don't keep a piece of paper just on the chance that you may need it "someday."
b) Don't always save every draft of a document. For most purposes the final version is sufficient.
c) Don't file multiple copies of the same document, unless justified.
d) The originator normally keeps copies of invoices and correspondence. Just because a document is sent to you doesn't mean that you are obliged to keep it indefinitely. If you need to see it again, ask the originator for another copy.
e) If, for example, records are scheduled for destruction after three years, don't store them for five years.
f) In general, records received from schools/institutes/centres/offices should be filed under the name of the originating school/institute/centre/office.
g) Some records may belong under more than one series or category. To handle this, file the records in one category and place a cross-reference note in the other. It is important to be consistent in deciding where to file records. Once information is filed in a given series and category, it should always be filed there.
h) Label and date all files.
i) Sort records prior to filing.
j) Use staples rather than paper clips in folders.
k) Discard envelopes if the return address is available on the document itself. Most phone messages, illegible notes, and routine acknowledgements can also be discarded.