PAUL Partnership Privacy Policy

OUR PRIVACY POLICY AT A GLANCE

1. **WHO WE ARE**: We are PAUL Partnership Limerick Company Limited by Guarantee. We are the multi-sectoral partnership company for Limerick City. We work in partnership for social and economic inclusion in Limerick City.

2. **WHAT WE USE YOUR DATA FOR**: We use your data collected in person or online to:
    - Contact you to respond to any queries or communications you may send us
    - Establish your eligibility for our various programmes and supports
    - Review how we assisted you so we can provide you with the best possible tailored supports
    - Share your name and contact details with third parties, with your agreement, so we can make referrals and appointments on your behalf
    - Produce statistics which will help us plan and improve our services
    - Provide our funders with data to assist them in providing a better national service
    - Provide you with information about our upcoming training courses, workshops, and events

3. **OUR LEGAL BASIS FOR PROCESSING YOUR DATA**: We are legally permitted to process your data based on the following grounds:
    - When you register for one of our services, **consent** is provided by you for us to process your data.
    - For some of our services, (e.g. Local Employment Service and Jobs Club), we are required to process your data in order for you to fulfil a **legal contract** with the Department of Employment Affairs and Social Protection (the Data Controller).

4. **WHO WE SHARE YOUR DATA WITH**: We will sometimes share your data with other service providers, namely:
    - For services and programmes where we are the Data Processor (e.g. the Local Employment Service, Jobs Club, Tús, Community Employment), we will share your data with the Data Controller (Department of Employment Affairs and Social Protection)
    - For services and programmes where we are the Data Controller (e.g. Social Inclusion and Community Activation Programme, ABC Start Right, Incredible Years), we may share your data with third parties in order to arrange referrals to other services. We will only do this with your consent. We may also share your data with our funders for audit and monitoring purposes.

5. **HOW LONG DO WE KEEP YOUR DATA**: The duration for which we keep your data will depend on the purposes for which we processed the data, and will be articulated to you when you first provide data. We commit to only keep data for the period of time for which it is required to be kept by us.

6. **YOUR RIGHTS**: You have the right to access, rectify, and in some cases, to delete your personal data.

We encourage you to read our full Privacy Policy below to understand in depth the manner in which we will use your personal data and your rights over your data.

Contents

BEFORE YOU START ……

There are some terms and definitions that we use throughout this policy. These are explained here:

Personal Data is any **information that can identify an individual person**. This includes a name, a postal address, email address, IP address, location data (for example, location data collected by a mobile phone), Personal Public Services Number (PPSN).

Sensitive Personal Data are 'special categories of personal data'. It refers to data relating to: race, ethnicity, political, religious or philosophical beliefs, health, sexual activity or orientation, trade union membership, genetic or biometric data, criminal record.

Data Processing is any operation, or set of operations, on personal data, including:

- Obtaining, recording, or keeping data
- Organising or altering the data
- Retrieving, consulting or using the data
- Disclosing the data to a third party
- Erasing or destroying data

It applies to both automated processing of data and manual processing of data. It applies to both hard copy and electronic data. Simply storing data is considered 'processing'.

Data Controller is the person/organisation who is responsible for keeping and using personal data. The data controller decides why and how data is processed.

Data Processor is the person/organisation who processes personal data but does not exercise responsibility or control over the personal data. A data processor processes personal data on behalf of a Data Controller.

Data Subject is the individual the personal data relates to. In an organisation, it includes both clients/customers and employees.

ABOUT PAUL PARTNERSHIP LIMERICK

PAUL Partnership Limerick Company Limited by Guarantee (referred to as PAUL Partnership) is the multi-sectoral partnership company which promotes social inclusion in Limerick City. We are an organisation made up of representatives of communities, state agencies, social partners, voluntary groups and elected representatives. Our mission is to work in partnership for social and economic inclusion and improved quality of life in Limerick City.

We deliver services and supports to individuals in Limerick City through a number of different programmes/services, some of which involve the processing of personal data. We also process data on our employees and on individuals applying for positions within PAUL Partnership.

ABOUT THIS POLICY

PAUL Partnership is committed to protecting your privacy. In this Privacy Policy, you will find all relevant information applicable to our use of our clients' and employees' personal data, regardless of the channel (programme/service) or means (online or in person) that you interact with us.

Our Privacy Policy outlines our commitment and procedures for adhering to the principles of the Data Protection Acts of 1988 and 2003 and other relevant statutory provisions, including the General Data Protection Regulation (GDPR) which came into effect on May 25th 2018.

All our data processing activity adheres to the following principles:

1. Obtain and process information fairly
2. Keep it only for one or more specified, explicit and lawful purposes
3. Use and disclose information only in ways compatible with these purposes
4. Keep it safe and secure
5. Keep it accurate, complete and up-to-date
6. Ensure it is adequate, relevant and not excessive
7. Retain for no longer than is necessary
8. Allow individual's access to their personal data, on request

The key principles under GDPR are:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

Our Privacy Policy recognises that you have the following rights under data protection law, although your ability to exercise these rights may be subject to certain conditions:

- The right to receive a copy of and/or access the personal data that we hold about you, together with other information about our processing of that personal data;
- The right to request that any inaccurate data that is held about you is corrected, or if we have incomplete information you may request that we update the information such that it is complete;
- The right, in certain circumstances, to request that we erase your personal data;
- The right, in certain circumstances, to request that we no longer process your personal data for particular purposes, or object to our use of your personal data or the way in which we process it;
- The right, in certain circumstances, to transfer your personal data to another organisation;
- The right to object to automated decision making and/or profiling;
- The right to complain to the Data Protection Commission.

DEFINITION AND PRINCIPLES OF CONFIDENTIALITY

All information that:

a) is or has been obtained during, or in the course of involvement, or has otherwise been acquired in trust due to involvement with the organisation,

b) relates particularly to the organisation's business, clients or that of other persons or bodies with whom we have dealings of any sort, and

c) has not been made public by, or with our authority,

is confidential, and (save in the course of our business or as required by law) Board Members/Employees shall not at any time, whether before or after the end of their involvement with PAUL Partnership, disclose such information in any form to any person without our written consent.

Board Members/Employees are expected to exercise care to keep safe all documentary or other material containing confidential information, and at the time of end of a individual's involvement with the organisation, or at any other time upon demand, return to the organisation any such material in their possession.

Information held by the organisation and not independently available to a third party cannot be disclosed without the individual's written consent and permission from the CEO.

LIMITS TO CONFIDENTIALITY

In exceptional circumstances the organisation may need to break confidentiality if they believe there is a real intent of serious harm or danger to either their client or another individual. Such circumstances may pertain to issues relating to self-harm, expression of suicidal thoughts, criminal

activity or child protection. In as far as is possible, in such cases, a full explanation will be given regarding the necessary procedures that may need to be taken.

ACCESS REQUESTS

- A key right for the individual is the right of access. Essentially this means that individuals have the right to access their personal data, if a valid request is made.
- Where PAUL Partnership is the Data Controller:
    - All data access requests should be submitted to the CEO and should be received in writing.
    - We will respond to requests for information within 30 days.
    - In order to ensure compliance with the time limit, the CEO will appoint the Senior Manager with responsibility for data protection to:
        - Check the validity of the access request and check that sufficient material has been supplied to definitively identify the individual.
        - Log the date of receipt of the valid request and to keep note of all steps taken to locate and collate data.
        - Establish whether there are any exemptions to data disclosure.
    - Data relating to a Third Party will be redacted unless consent to disclose is given by the Third Party.
- Where PAUL Partnership is the Data Processor:
    - The individual will be directed to submit their request directly to the Data Controller.

PERSONAL DATA BREACH NOTIFICAITON AND INVESTIGATION

A 'personal data breach' refers to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

In the event of a suspected data breach, we will take the following steps:

- The CEO will be informed of the suspected breach as soon as it becomes known.
- Within 72 hours of becoming aware of a suspected breach, notification will be submitted to:
    - The Data Protection Commission using the National Breach Notification Form – in situations where we are the Data Controller.
    - The relevant Data Controller – in situations where we are the Data Processor.
- The CEO will appoint the Senior Manager with responsibility for data protection to undertake a full investigation of the incident and compile a written report. The investigation will determine if a breach has occurred, and if so, the circumstances of the breach. The investigation will also determine the number of data subjects involved, the impact of the breach on them, the steps to inform those affected, the measures taken to mitigate the impact, and the measures taken to prevent a reoccurrence of the incident.

DATA SECURITY

Technical and organisational security measures are in place to protect your personal data. Security measures are subject to technical progress and development. We may update or modify the

security measures from time to time to ensure the continued security of your data. Current measures are outlined in Appendix B.

DATA DELETION

At the end of the stated data retention period, personal data will be deleted via confidential shredding and/or via secure deletion of electronic records.

TRAINING

All staff members receive training in relation to data protection principles and procedures as part of their Induction.

SPECIFIC RESPONSIBILITIES

PAUL Partnership is responsible for ensuring that Board Members and staff involved in dealing with confidential information and personal data receive appropriate training, supervision and support regarding this policy. All staff sign a Data Protection and Confidentiality Agreement as part of their contract of employment.

The CEO is responsible for ensuring that a copy of this document is available to all Board Members and staff and is available to users of our services. It is the responsibility of the CEO to ensure that staff and Board Members receive training as necessary.

Individual staff and Board members are required to act in accordance with this policy, failure to do so will be considered as an act of gross misconduct and will result in disciplinary action.

SCOPE OF POLICY

This policy applies to all individuals who:

i. engage with PAUL Partnership's services and programmes in a **personal capacity**
ii. **are employed** by PAUL Partnership, or
iii. sit on the **Board** of Management.

It applies only to personal and sensitive data that can identify the data subject concerned. In this Policy, we answer the following:

- Who is the data controller for your data?
- What personal and sensitive data do we collect?
- What is our purpose for collecting and processing your personal data?
- What is the legal basis for collecting and processing your data?
- Do we share your data with Third Parties?
- Do we use for data for direct marketing purposes?
- How long do we keep your data?
- What are our security arrangements for protecting your data?
- What are your data protection rights?

Depending on how you engage with us, or the means (in person or online), different data is collected and processed for different purposes. This Privacy Policy details this information for each of the following areas:

1. Social Inclusion and Community Activation Programme (known as SICAP)
2. Local Employment Service (LES)
3. Jobs Club
4. Tús
5. Community Employment – Community Outreach Team
6. Community Employment – Childcare Training and Development Programme
7. Incredible Years Limerick
8. ABC Start Right
9. Fit for Work and Life
10. Employee and HR data
11. Website data

CHANGES TO THE PRIVACY POLICY

We may amend the information contained in this Privacy Policy when we consider this appropriate and when we have new programmes and services which involve the processing of personal data. We will notify you by various procedures (for example, through a pop-up or notice on our website) or by email when the change in question is relevant to your privacy, for you to be able to review the changes, assess them and, as the case may be, object or unsubscribe from a service. In any case, we suggest that you review this Privacy Policy from time to time in case minor changes are made.

CONTACT DETAILS

If you have any questions regarding the above statement please contact PAUL Partnership as follows:

The CEO,
PAUL Partnership,
Unit 25a,
Tait Business Centre,
Dominic Street,
Limerick.

Email: dataprotection@paulpartnership.ie
Tel: 061 419388

****

SOCIAL INCLUSION AND COMMUNITY ACTIVATION PROGRAMME (SICAP)

Who is the Data Controller?	The Data Controller is: PAUL Partnership Limerick Company Limited by Guarantee (CLG) (referred to as PAUL Partnership) Unit 25a, Tait Business Centre, Dominic Street, Limerick Tel: 061 419388; Email: info@paulpartnership.ie
What personal data do we collect?	Name, address, telephone number, email, date of birth and/or age group, education level, employment status, nationality, immigration status, Personal Public Services Number
What sensitive data do we collect?	Ethnicity, Disability status
What is our purpose for collecting and processing your personal data?	• To establish if you are eligible for programme supports • To contact you to provide ongoing and follow up supports as part or our service delivery • To register you for SICAP-funded courses • To share your name and contact details with other service providers, as agreed with you, so we can make referrals and appointments on your behalf • To provide you with information on upcoming courses, workshops and events that may be of interest to you • To review how we assisted you so we can provide you with the best possible tailored supports • To produce statistics on programme outcomes which will help us plan and improve our services • To facilitate any audits on our services/programmes by our funders
What is the legal basis for collecting and processing your data?	We collect and process your personal data based on your **consent** for us to do so. When you register for a SICAP activity or service, you are informed about the data processing activities of the programme. We will only proceed if you willingly give informed consent.
Do we use your data for direct marketing purposes?	We only use your data for direct marketing purposes if you have provided consent (by email, text, or in writing) to be included in any direct marketing correspondence we may have about our upcoming courses, workshops or events.
Do we share your data with Third Parties?	We may share your data with Third Parties in order to arrange follow up appointments or referrals to other service providers (e.g. Education and Training Board, Citizen's Information Centre). This is agreed with you in advance. On occasion, your data may be shared with an Auditor. The purpose of this is to enable our services to be audited by our funder – the Department of Rural and Community Development. Your data may also be shared with Pobal IT

	system administrators who manage the monitoring system on behalf of the programme funder.
How long do we keep your data?	The information you provide us with will be stored for the duration of time you engage with the programme and for a period of seven years after you exit the programme.
What are our security arrangements for protecting your data?	Your personal data is stored on a secure computer database which is accessed only by staff authorised to do so for the purpose of managing and delivering the programme. Internal ICT systems are fully protected by anti-virus and encryption software. Any data stored on hard copy is stored in locked filing cabinets which are only accessed by those with authorisation to do so.
What are your data protection rights?	Under the Irish Data Protection Acts and the EU General Data Protection Regulation (GDPR) 2018, you have the right to: • Request a copy of your personal information at any time • Request that any inaccurate data is amended • Withdraw your consent to provide information and have your data deleted. You can do this by contacting us on dataprotection@paulpartnership.ie. We will respond to your request within 30 days.

LOCAL EMPLOYMENT SERVICE

Who is the Data Controller?	The Data Controller is: Department of Employment Affairs and Social Protection (DEASP) - Data Protection Office Goldsmith House Pearse St Dublin 2 dpo@welfare.ie Further information about the Data Protection Policies of the DEASP can be found on: http://www.welfare.ie/en/Pages/Data-Protection-DEASP.aspx
Who is the Data Processor?	The Data Processor is: PAUL Partnership Limerick Company Limited by Guarantee (CLG) (referred to as PAUL Partnership) Unit 25a, Tait Business Centre, Dominic Street, Limerick Tel: 061 419388; Email: info@paulpartnership.ie We (PAUL Partnership) collect and process your data on behalf of the Data Controller.

What personal data do we collect?	Name, address, telephone number, email, date of birth, education/ training history, employment/work history, hobbies/ interests, references, Personal Public Services Number (PPSN), immigration status (where applicable), current/new education and training status, current/new employment status.
What sensitive data do we collect?	Ethnicity, Disability
What is our purpose for collecting and processing your personal data?	• To establish if you are eligible for the service (if necessary) • To assist you in progressing to employment, training, or education • To contact you to provide ongoing and follow up supports as part or our service delivery • To provide information to the Department of Employment Affairs and Social Protection about the nature and outcome of your engagement with the service • To share your name and contact details with other service providers and/or employers, as agreed with you, so we can make referrals and appointments on your behalf • To review how we assisted you so we can provide you with the best possible tailored supports • To produce statistics which will help us plan and improve our services • To facilitate any audits on our services/programmes by our funders
What is the legal basis for collecting and processing your data?	If you are referred to our service by the Department of Employment Affairs and Social Protection, we collect and process your personal data in order to fulfil the **contract** between you and the Data Controller (Department of Employment Affairs and Social Protection (DEASP). The primary **legal basis** enabling the DEASP to collect your personal data is the Social Welfare Consolidation Act 2005 (as amended). If you engage with our service on a 'walk in' basis, we collect and process your personal data based on your **consent** for us to do so. When you register for the LES, you are informed about the data processing activities of the service. We will only proceed if you willingly give informed consent.
Do we use your data for direct marketing purposes?	We only use your data for direct marketing purposes if you have provided consent (by email, text, or in writing) to be included in any direct marketing correspondence we may have about our upcoming courses, workshops or events.
Do we share your data with Third Parties?	We share your data with the Data Controller – Department of Employment Affairs and Social Protection. We may share your data with Third Parties in order to arrange follow up appointments or referrals to other service providers and other employers.
How long do we keep your data?	The information you provide us with will be stored by us for the duration of time you engage with the service and for a period of 1 year after you exit the service.

What are our security arrangements for protecting your data?	Your personal data is stored on a secure computer database which is accessed only by those authorised to do so for the purpose of monitoring and delivering the service. This includes authorised staff of the Data Controller (Department of Employment Affairs and Social Protection). Internal ICT systems are fully protected by anti-virus and encryption software. Any data stored on hard copy is stored in locked filing cabinets which are only accessed by those with authorisation to do so.
What are your data protection rights?	Under the Irish Data Protection Acts and the EU General Data Protection Regulation (GDPR) 2018, you have a right to request a copy of your personal information at any time, and to have inaccurate data rectified. You can do so by contacting the Data Controller on: Data Protection Officer Department of Employment Affairs and Social Protection Goldsmith House Pearse St Dublin 2 dpo@welfare.ie Under GDPR, the Data Controller will normally have 30 days to process your request.

JOBS CLUB

Who is the Data Controller?	The Data Controller is: Department of Employment Affairs and Social Protection - Data Protection Office Goldsmith House Pearse St Dublin 2 dpo@welfare.ie Further information about the Data Protection Policies of the DEASP can be found on: http://www.welfare.ie/en/Pages/Data-Protection-DEASP.aspx
Who is the Data Processor?	The Data Processor is: PAUL Partnership Limerick Company Limited by Guarantee (CLG) (referred to as PAUL Partnership) Unit 25a, Tait Business Centre, Dominic Street, Limerick Tel: 061 419388; Email: info@paulpartnership.ie We (PAUL Partnership) collect and process your data on behalf of the Data Controller.

What personal data do we collect?	Name, address, telephone number, email, date of birth, education/ training history, employment/work history, hobbies/ interests, references, Personal Public Services Number (PPSN), immigration status (where applicable), current/new education and training status, current/new employment status.
What sensitive data do we collect?	Ethnicity, Disability
What is our purpose for collecting and processing your personal data?	• To establish if you are eligible for the service (if necessary) • To assist you in progressing to employment, training, or education • To contact you to provide ongoing and follow up supports as part or our service delivery • To provide information to the Department of Employment Affairs and Social Protection about the nature and outcome of your engagement with the service • To share your name and contact details with other service providers and/or employers, as agreed with you, so we can make referrals and appointments on your behalf • To review how we assisted you so we can provide you with the best possible tailored supports • To produce statistics which will help us plan and improve our services • To facilitate any audits on our services/programmes by our funders
What is the legal basis for collecting and processing your data?	If you are referred to our service by the Department of Employment Affairs and Social Protection, we collect and process your personal data in order to fulfil the **contract** between you and the Data Controller (Department of Employment Affairs and Social Protection (DEASP). The primary **legal basis** enabling the DEASP to collect your personal data is the Social Welfare Consolidation Act 2005 (as amended). If you engage with our service on a 'walk in' basis, we collect and process your personal data based on your **consent** for us to do so. When you register for the Jobs Club, you are informed about the data processing activities of the service. We will only proceed if you willingly give informed consent.
Do we use your data for direct marketing purposes?	We only use your data for direct marketing purposes if you have provided consent (by email, text, or in writing) to be included in any direct marketing correspondence we may have about our upcoming courses, workshops or events.
Do we share your data with Third Parties?	We share your data with the Data Controller – Department of Employment Affairs and Social Protection. We share your data with Third Parties in order to arrange follow up appointments or referrals to other service providers and/or employers.
How long do we keep your data?	The information you provide us with will be stored by us for the duration of time you engage with the service and for a period of 1 year after you exit the service.
What are our security	Your personal data is stored on a secure computer database which is accessed only by those authorised to do so for the purpose of managing and delivering

arrangements for protecting your data?	the service. This includes authorised staff of the Data Controller (Department of Employment Affairs and Social Protection). Internal ICT systems are fully protected by anti-virus and encryption software. Any data stored on hard copy is stored in locked filing cabinets which are only accessed by those with authorisation to do so.
What are your data protection rights?	Under the Irish Data Protection Acts and the EU General Data Protection Regulation (GDPR) 2018, you have a right to request a copy of your personal information at any time, and to have inaccurate data rectified. You can do so by contacting the Data Controller on: Data Protection Officer Department of Employment Affairs and Social Protection Goldsmith House Pearse St Dublin 2 dpo@welfare.ie Under GDPR, the Data Controller will normally have 30 days to process your request.

TÚS

Who is the Data Controller?	The Data Controller is: Department of Employment Affairs and Social Protection - Data Protection Office Goldsmith House Pearse St Dublin 2 dpo@welfare.ie Further information about the Data Protection Policies of the DEASP can be found on: http://www.welfare.ie/en/Pages/Data-Protection-DEASP.aspx
Who is the Data Processor?	The Data Processor is: PAUL Partnership Limerick Company Limited by Guarantee (CLG) (referred to as PAUL Partnership) Unit 25a, Tait Business Centre, Dominic Street, Limerick Tel: 061 419388; Email: info@paulpartnership.ie We (PAUL Partnership) collect and process your data on behalf of the Data Controller.
What personal data do we collect?	Name, address, telephone number, email, date of birth, education/ training history, employment/work history, hobbies/ interests, references, Personal Public Services Number (PPSN), current/new employment status.

	If you are employed by us on the Tús Programme, we also collect bank account details, hours worked, parental/force majeure leave, tax records, health and safety records, DEASP payment details, spouse/partner PPSN (if on same DEASP claim), name and date of birth of children (if required for DEASP claim), next-of-kin details. We may also collect medical records where relevant.
What sensitive data do we collect?	Criminal record (if identified through a required Garda Vetting check)
What is our purpose for collecting and processing your personal data?	• To identify and arrange an appropriate work placement for you in a host community organisation • To process the payment of your salary • To maintain personnel records in line with employment legislation • To provide information to the Department of Employment Affairs and Social Protection about the nature and outcome of your engagement with the service • To produce statistics which will help us plan and improve our services • To facilitate any audits on our services/programmes by our funders
What is the legal basis for collecting and processing your data?	If you are referred to our service by the Department of Employment Affairs and Social Protection, we collect and process your personal data in order to fulfil the **contract** between you and the Data Controller (Department of Employment Affairs and Social Protection (DEASP), and to fulfil the **contract** between PAUL Partnership and the DEASP to implement the Tús programme. The primary **legal basis** enabling the DEASP to collect your personal data is the Social Welfare Consolidation Act 2005 (as amended). If you are employed by us via the Tús Programme, our legal basis for processing your personal data is to enable the fulfilment of an employment **contract** between you and PAUL Partnership and to meet employment and revenue **legislation**.
Do we use your data for direct marketing purposes?	We only use your data for direct marketing purposes if you have provided consent (by email, text, or in writing) to be included in any direct marketing correspondence we may have about our upcoming courses, workshops or events.
Do we share your data with Third Parties?	We share your data with the Data Controller – Department of Employment Affairs and Social Protection. We share relevant data with community organisations in order to arrange a work placement for you. For some positions, we share relevant data with Early Childhood Ireland in order to process your Garda Vetting prior to commencement of employment. We share the details of the Garda Vetting outcome with the relevant community organisation.
How long do we keep your data?	If you are employed with us through the Tús Programme, the information you provide us with will be stored for the duration of time you are employed with

	us. In order to meet employment and revenue legislative obligations we are required to retain some personal data for a longer period of time. This is detailed on our Data Retention Policy – Employee Records. In the event that you do not secure a work placement, we will keep any data collected during interview/recruitment for a period of 1 year post interview.
What are our security arrangements for protecting your data?	Your personal data is stored on a secure computer database which is accessed only by those authorised to do so for the purposes of managing and delivering the programme. This includes authorised staff of the Data Controller (Department of Employment Affairs and Social Protection). Internal ICT systems are fully protected by anti-virus and encryption software. Any data stored on hard copy is stored in locked filing cabinets which are only accessed by those with authorisation to do so.
What are your data protection rights?	Under the Irish Data Protection Acts and the EU General Data Protection Regulation (GDPR) 2018, you have a right to request a copy of your personal information at any time, and to have inaccurate data rectified. You can do so by contacting the Data Controller on: Data Protection Officer Department of Employment Affairs and Social Protection Goldsmith House Pearse St Dublin 2 dpo@welfare.ie Under GDPR, the Data Controller will normally have 30 days to process your request.

COMMUNITY EMPLOYMENT (CE) – COMMUNITY OUTREACH TEAM

Who is the Data Controller?	The Data Controller is: Department of Employment Affairs and Social Protection - Data Protection Office Goldsmith House Pearse St Dublin 2 dpo@welfare.ie Further information about the Data Protection Policies of the DEASP can be found on: http://www.welfare.ie/en/Pages/Data-Protection-DEASP.aspx
Who is the Data Processor?	The Data Processor is: PAUL Partnership Limerick Company Limited by Guarantee (CLG) (referred to as PAUL Partnership)

	Unit 25a, Tait Business Centre, Dominic Street, Limerick Tel: 061 419388; Email: info@paulpartnership.ie We (PAUL Partnership) collect and process your data on behalf of the Data Controller.
What personal data do we collect?	Name, address, telephone number, email, date of birth, education/ training history, employment/work history, hobbies/interests, references, Personal Public Services Number (PPSN), current/new employment status. For some positions, we may also require proof of address and copy of photo ID . If you are employed by us on the CE Community Outreach Team, we also collect bank account details, hours worked, parental/force majeure leave, tax records, health and safety records, next of kin details. We may also collect medical records where relevant.
What sensitive data do we collect?	Criminal records (if identified through a required Garda Vetting check)
What is our purpose for collecting and processing your personal data?	• To identify and arrange an appropriate work placement for you within PAUL Partnership or within a community partner organisation • To process the payment of your salary • To maintain personnel records in line with employment legislation • To assist you to develop Individual Learning Plans (ILPs) • To provide information to the Department of Employment Affairs and Social Protection about the nature and outcome of your engagement with the service • To produce statistics which will help us plan and improve our services • To facilitate any audits on our services/programmes by our funders
What is the legal basis for collecting and processing your data?	If you are referred to our service by the Department of Employment Affairs and Social Protection, we collect and process your personal data in order to fulfil the **contract** between you and the Data Controller (Department of Employment Affairs and Social Protection (DEASP), and to fulfil the **contract** between PAUL Partnership and the DEASP to implement the CE programme. The primary **legal basis** enabling the DEASP to collect your personal data is the Social Welfare Consolidation Act 2005 (as amended). If you are employed by us on the CE Community Outreach Team, our legal basis for processing your personal data is to enable the fulfilment of an employment **contract** between you and PAUL Partnership and to meet employment and revenue **legislation**.
Do we use your data for direct marketing purposes?	We only use your data for direct marketing purposes if you have provided consent (by email, text, or in writing) to be included in any direct marketing correspondence we may have about our upcoming courses, workshops or events.
Do we share	We share your data with the Data Controller – Department of Employment

your data with Third Parties?	Affairs and Social Protection. We may share relevant data with a community partner organisation in order to arrange a work placement for you, or with an Education Provider in order to register a place for you on a course. For some positions, we share relevant data with Early Childhood Ireland in order to process your Garda Vetting prior to commencement of employment. We share the details of the Garda Vetting outcome with the relevant community organisation.
How long do we keep your data?	If you are employed with us on the CE Community Outreach Team, the information you provide us with will be stored for the duration of time you are employed with us. Individual Learning Plans are stored for a duration of 1 year post Programme exit. In order to meet employment and revenue legislative obligations we are required to retain some personal data for a longer period of time. This is detailed on our Data Retention Policy – Employee Records. In the event that you do not secure a work placement with us, we will keep any data collected during interview/recruitment for a period of 1 year post interview.
What are our security arrangements for protecting your data?	Your personal data is stored on a secure computer database which is accessed only by those authorised to do so for the purposes of managing and delivering the programme. This includes authorised staff of the Data Controller (Department of Employment Affairs and Social Protection). Internal ICT systems are fully protected by anti-virus and encryption software. Any data stored on hard copy is stored in locked filing cabinets which are only accessed by those with authorisation to do so.
What are your data protection rights?	Under the Irish Data Protection Acts and the EU General Data Protection Regulation (GDPR) 2018, you have a right to request a copy of your personal information at any time, and to have inaccurate data rectified. You can do so by contacting the Data Controller on: Data Protection Officer Department of Employment Affairs and Social Protection Goldsmith House Pearse St Dublin 2 dpo@welfare.ie Under GDPR, the Data Controller will normally have 30 days to process your request.

COMMUNITY EMPLOYMENT (CE) – CHILDCARE TRAINING AND DEVELOPMENT PROGRAMME

Who is the Data Controller?	The Data Controller is: Department of Employment Affairs and Social Protection - Data Protection Office Goldsmith House Pearse St Dublin 2 dpo@welfare.ie Further information about the Data Protection Policies of the DEASP can be found on: http://www.welfare.ie/en/Pages/Data-Protection-DEASP.aspx
Who is the Data Processor?	The Data Processor is: PAUL Partnership Limerick Company Limited by Guarantee (CLG) (referred to as PAUL Partnership) Unit 25a, Tait Business Centre, Dominic Street, Limerick Tel: 061 419388; Email: info@paulpartnership.ie We (PAUL Partnership) collect and process your data on behalf of the Data Controller.
What personal data do we collect?	Name, address, telephone number, email, date of birth, gender, education/ training history, employment/work history, hobbies/interests, references, Personal Public Services Number (PPSN), current/new employment status, proof of address, copy of photo ID, medical card number (where applicable) If you are employed by us on the CE Childcare Programme, we also collect bank account details, hours worked, parental/force majeure leave, tax records, health and safety records, next of kin details. We may also collect medical records where relevant.
What sensitive data do we collect?	Criminal records (if identified through the Garda Vetting process).
What is our purpose for collecting and processing your personal data?	• To identify and arrange an appropriate work placement for you in a host community childcare setting • To register a place for you on a FETAC Level 5 or 6 Childcare training course • To process the payment of your salary • To maintain personnel records in line with employment legislation • To assist you to develop Individual Learning Plans (ILPs) • To provide information to the Department of Employment Affairs and Social Protection about the nature and outcome of your engagement with the service • To produce statistics which will help us plan and improve our services

	• To facilitate any audits on our services/programmes by our funders
What is the legal basis for collecting and processing your data?	If you are referred to our service by the Department of Employment Affairs and Social Protection, we collect and process your personal data in order to fulfil the **contract** between you and the Data Controller (Department of Employment Affairs and Social Protection (DEASP), and to fulfil the **contract** between PAUL Partnership and the DEASP to implement the programme. The primary **legal basis** enabling the DEASP to collect your personal data is the Social Welfare Consolidation Act 2005 (as amended). If you are employed by us via the CE Childcare Programme, our legal basis for processing your personal data is to enable the fulfilment of an employment **contract** between you and PAUL Partnership and to meet employment and revenue **legislation**.
Do we use your data for direct marketing purposes?	We only use your data for direct marketing purposes if you have provided consent (by email, text, or in writing) to be included in any direct marketing correspondence we may have about our upcoming courses, workshops or events.
Do we share your data with Third Parties?	We share your data with the Data Controller – Department of Employment Affairs and Social Protection. We share relevant data with community childcare settings in order to arrange a work placement for you. We also share relevant data with an education provider in order to register your place on the relevant Childcare training modules. We share relevant data with Early Childhood Ireland in order to process your Garda Vetting prior to commencement of employment. We share the details of the Garda Vetting outcome with the relevant community organisation.
How long do we keep your data?	If you are employed with us through the CE Childcare Programme, the information you provide us with will be stored for the duration of time you are employed with us. Individual Learning Plans are stored for a duration of 1 year post Programme exit. In order to meet employment and revenue legislative obligations we are required to retain some personal data for a longer period of time. This is detailed on our Data Retention Policy – Employee Records. In the event that you do not secure a work placement with us, we will keep any data collected during interview/recruitment for a period of 1 year post interview.
What are our security arrangements for protecting your data?	Your personal data is stored on a secure computer database which is accessed only by those authorised to do so for the purposes of managing and delivering the programme. This includes authorised staff of the Data Controller (Department of Employment Affairs and Social Protection). Internal ICT systems are fully protected by anti-virus and encryption software. Any data stored on hard copy is stored in locked filing cabinets which are only accessed by those with authorisation to do so.

What are your data protection rights?	Under the Irish Data Protection Acts and the EU General Data Protection Regulation (GDPR) 2018, you have a right to request a copy of your personal information at any time, and to have inaccurate data rectified. You can do so by contacting the Data Controller on: Data Protection Officer Department of Employment Affairs and Social Protection Goldsmith House Pearse St Dublin 2 dpo@welfare.ie Under GDPR, the Data Controller will normally have 30 days to process your request.

INCREDIBLE YEARS (IY) LIMERICK

Who is the Data Controller?	The Data Controller is: PAUL Partnership Limerick Company Limited by Guarantee (CLG) (referred to as PAUL Partnership) Unit 25a, Tait Business Centre, Dominic Street, Limerick Tel: 061 419388; Email: info@paulpartnership.ie
What personal data do we collect?	***Incredible Years Group Leaders***: Name, Telephone, Employer, Qualifications, video recording of Group Leader during programme delivery ***Incredible Years Participants***: **Teachers**: Name, Employer, Qualifications **Parents**: Voice recorded during programme delivery sessions; images and names where consent is provided for photographs to be taken **Children**: Voice recorded during programme delivery sessions; images and names where consent is provided for photographs to be taken.
What sensitive data do we collect?	Health (dietary or accessibility requirements)
What is our purpose for collecting and processing your personal data?	• To organise and co-ordinate the delivery of Incredible Years programmes and training programmes for IY Group Leaders • To monitor quality assurance and fidelity to the programme during programme delivery • To review quality of programme delivery as part of the Group Leader accreditation process • To produce statistics which will help us plan and improve our services
What is the legal basis for	We collect and process your personal data based on your **consent** for us to do so. When you register for an Incredible Years Programme, you are informed

collecting and processing your data?	about the data processing activities of the programme. We will only proceed if you willingly give informed consent.
Do we use your data for direct marketing purposes?	We only use your data for direct marketing purposes if you have provided consent (by email, text, or in writing) to be included in any direct marketing correspondence we may have about our upcoming courses, workshops or events.
Do we share your data with Third Parties?	Video recordings of Group Leaders delivering IY Programmes are shared with Incredible Years Seattle, and may be shared with other Group Leaders during Peer Support Sessions. Relevant personal data of Group Leaders (e.g. name, contact details, qualifications) applying for Accreditation are shared with Incredible Years Seattle.
How long do we keep your data?	We retain personal data for the period of time required to complete Incredible Years accreditation and training processes.
What are our security arrangements for protecting your data?	Your personal data is stored on secure computer files which are accessed only by those authorised to do so, i.e., programme staff. Internal ICT systems are fully protected by anti-virus and encryption software. Any data stored on hard copy is stored in locked filing cabinets which are only accessed by those with authorisation to do so.
What are your data protection rights?	Under the Irish Data Protection Acts and the EU General Data Protection Regulation (GDPR) 2018, you have a right to request a copy of your personal data at any time, and to have inaccurate data rectified. You can do so by contacting us on dataprotection@paulpartnership.ie . You also have the right to withdraw your consent to provide any of the information requested and have your data deleted. You can do this by contacting us on dataprotection@paulpartnership.ie. We will respond to your request within 30 days.

ABC START RIGHT

Who is the Data Controller?	The Data Controller is: PAUL Partnership Limerick Company Limited by Guarantee (CLG) (referred to as PAUL Partnership) Unit 25a, Tait Business Centre, Dominic Street, Limerick Tel: 061 419388; Email: info@paulpartnership.ie
What personal data do we collect?	**Early Years Staff:** Name, telephone, email, employer, qualification, (Qualifications collected in respect of staff participating in training activities only). **Parents:** Name, address, telephone

	Children: Name, date of birth, clinical speech and language assessment results. Assessment results collected in respect of children participating in Little Voices programme only.
What sensitive data do we collect?	Learning, development and health data on children participating in the Little Voices Talkboost and Early Talkboost Programmes may occasionally be collected. Criminal records (if identified through the Garda Vetting process).
What is our purpose for collecting and processing your personal data?	• To organise and co-ordinate the delivery of workshops and events • To connect you to the services of our Community Wraparound partners and/or other services • To inform early years staff and parents about upcoming workshops, programmes and events • To monitor and track progress of programme participants • To produce statistics which will help us plan and improve our services
What is the legal basis for collecting and processing your data?	We collect and process your personal data based on your **consent** for us to do so. Children's personal data is processed on the basis of consent provided by their parent or legal guardian. When you register with the ABC Start Right programme, you are informed about the data processing activities of the programme. We will only proceed if you willingly give informed consent.
Do we use your data for direct marketing purposes?	We only use your data for direct marketing purposes if you have provided consent (by email, text, or in writing) to be included in any direct marketing correspondence we may have about our upcoming courses, workshops or events.
Do we share your data with Third Parties?	We share your data with our Community Wraparound partners and other service providers for the purpose of supporting you to connect with relevant services. Child clinical speech and language assessment data is shared with the HSE. We share relevant data with Early Childhood Ireland in order to process Garda Vetting. We share the details of the Garda Vetting outcome with the relevant community organisation.
How long do we keep your data?	We keep your data for the duration of the programme. Data shared with the HSE is retained in line with the HSE Data Retention Policy.
What are our security arrangements for protecting your data?	Your personal data is stored on secure computer files which are accessed only by those authorised to do so, i.e., programme staff. Internal ICT systems are fully protected by anti-virus and encryption software. Any data stored on hard copy is stored in locked filing cabinets which are only accessed by those with authorisation to do so.
What are your data protection	Under the Irish Data Protection Acts and the EU General Data Protection Regulation (GDPR) 2018, you have a right to request a copy of your personal

rights?	data at any time, and to have inaccurate data rectified. You can do so by contacting us on dataprotection@paulpartnership.ie. You also have the right to withdraw your consent to provide any of the information requested and have your data deleted. You can do this by contacting us on dataprotection@paulpartnership.ie. We will respond to your request within 30 days.

FIT FOR WORK AND LIFE

Who is the Data Controller?	The Data Controller is: PAUL Partnership Limerick Company Limited by Guarantee (CLG) (referred to as PAUL Partnership) Unit 25a, Tait Business Centre, Dominic Street, Limerick Tel: 061 419388; Email: info@paulpartnership.ie
What personal data do we collect?	Name, telephone, email of programme participants
What sensitive data do we collect?	None
What is our purpose for collecting and processing your personal data?	• To organise and co-ordinate the delivery of training programmes • To monitor and evaluate impact of programme delivery • To produce statistics which will help us plan and improve our services
What is the legal basis for collecting and processing your data?	We collect and process your personal data based on your **consent** for us to do so. When you register for a Fit for Work and Life programme, you are informed about the data processing activities of the programme. We will only proceed if you willingly give informed consent.
Do we use your data for direct marketing purposes?	We only use your data for direct marketing purposes if you have provided consent (by email, text, or in writing) to be included in any direct marketing correspondence we may have about our upcoming courses, workshops or events.
Do we share your data with Third Parties?	No. *Anonymised* evaluation and demographic data is shared with the Irish Cancer Society.
How long do we keep your data?	We keep your personal data for the duration of the programme. Signed attendance sheets are retained for a period of 7 years (when co-funded under SICAP).
What are our	Your personal data is stored on secure computer files which are accessed only

security arrangements for protecting your data?	by those authorised to do so, i.e., programme staff. Internal ICT systems are fully protected by anti-virus and encryption software. Any data stored on hard copy is stored in locked filing cabinets which are only accessed by those with authorisation to do so.
What are your data protection rights?	Under the Irish Data Protection Acts and the EU General Data Protection Regulation (GDPR) 2018, you have a right to request a copy of your personal data at any time, and to have inaccurate data rectified. You can do so by contacting us on dataprotection@paulpartnership.ie. You also have the right to withdraw your consent to provide any of the information requested and have your data deleted. You can do this by contacting us on dataprotection@paulpartnership.ie. We will respond to your request within 30 days.

EMPLOYEE AND HUMAN RESOURCES

Who is the Data Controller?	The Data Controller is: PAUL Partnership Limerick Company Limited by Guarantee (CLG) (referred to as PAUL Partnership) Unit 25a, Tait Business Centre, Dominic Street, Limerick Tel: 061 419388; Email: info@paulpartnership.ie
What personal data do we collect?	Name, Address, Telephone, Email, Date of Birth, Personal Public Services Number, Bank Account details, hours worked, parental/force majeure leave, tax records, health and safety records, next of kin details, motor insurance details, performance review notes. We may also collect medical records where relevant. Education/ training history, employment/work history, hobbies/interests, references collected for all job applicants. Proof of address and copy of photo ID collected from successful applicants to positions that require Garda Vetting.
What sensitive data do we collect?	Trade Union membership – where subscription is deducted from the payroll. Criminal record – if identified through a Garda Vetting process
What is our purpose for collecting and processing your personal data?	• To complete a recruitment process • To enable payment of salary • To enable administration of pension • To maintain personnel and HR data in line with employment and revenue legislation • To support training and professional development of employees • To investigate employee complaints, grievance issues, health and safety incidents

	• To contact employee next-of-kin in the event of an emergency • To provide employee references to third parties upon request
What is the legal basis for collecting and processing your data?	Our legal basis for processing your personal data is to enable the fulfilment of an employment **contract** between you and PAUL Partnership, to meet employment and revenue **legislation**, and where relevant, to protect legitimate business interests.
Do we use your data for direct marketing purposes?	No
Do we share your data with Third Parties?	We may share relevant data with the following: • Our funders for audit purposes • Our financial auditors • Revenue Commissioners • Department of Employment Affairs and Social Protection • Legal and insurance representatives • Workplace Relations Commission • Third parties who submit a reference request on behalf of a previous or existing employee.
How long do we keep your data?	Under employment and revenue legislation, we are legally required to keep certain data for a specified period of time. This is outlined in detail in our *Employee and HR Data Retention Policy.* Data for employees funded through specific programmes may be required to be retained for a longer period of time. Relevant data will be retained for which ever period of time is longer. (e.g. working time records are required by the Organisation of Working Time Act 1997 to be retained for a minimum of 3 years; but a specific programme may require this data to be retained for 5 years post the end of the programme. In this case, the employee data will be retained for the longer period of time).
What are our security arrangements for protecting your data?	Your personal data is stored on secure computer files which are accessed only by those authorised to do so, i.e., CEO, HR support, payroll staff (access to relevant data only). Internal ICT systems are fully protected by anti-virus and encryption software. Any data stored on hard copy is stored in locked filing cabinets which are only accessed by those with authorisation to do so.
What are your data protection rights?	Under the Irish Data Protection Acts and the EU General Data Protection Regulation (GDPR) 2018, you have a right to request a copy of your personal data at any time, and to have inaccurate data rectified. You can do so by contacting us on dataprotection@paulpartnership.ie. Employees are responsible for ensuring that they inform the relevant section (HR admin, payroll) of changes in personal details, e.g. change of address. Section Heads must inform the relevant section (HR admin, payroll) of changes in employees' personal details, e.g. change of hours work, completion of contract, promotion etc).

PAUL PARTNERSHIP WEBSITE PRIVACY STATEMENT

The following policy is only in effect for the web pages of www.paulpartnership.ie.

The purpose of this Website Privacy Statement is to outline how we deal with any personal data you provide to us while visiting our website. Any external links to other websites are clearly identifiable as such, and we are not responsible for the content or the privacy policies of these other websites. While we take care of the safety of information on our website on an ongoing basis, if you are not happy with this Privacy Statement you should not use our website.

What information are we collecting and how are we collecting it?

Every computer connected to the internet is given a domain name and a set of numbers that serve as that computer's 'Internet Protocol' IP address. When a visitor requests a page from www.paulpartnership.ie, our web server automatically recognises that visitor's domain name and IP address from which you have accessed our site. We use this information to examine our traffic in aggregate, but do not collect and evaluate this information for individuals.

What other information do we request?

We may also request your name and e-mail address for the following purposes:

- To contact you if required to respond to any communications you might send to us.
- To provide you with a subscription to an email newsletter.
- To contact selected PAUL Partnership staff that you have requested to be contacted on your behalf.

Whenever we request the identity of a visitor, we will clearly indicate the purpose of the inquiry before the information is requested.

What are cookies?

From time to time, www.paulpartnership.ie may send a 'cookie' to your computer. A cookie is a small piece of data that is sent to your browser from a web server and stored on your computer's hard drive. A cookie can't read off your hard disk or read cookie files created by other sites. Cookies do not damage your system. We use cookies to identify which areas of www.paulpartnership.ie you have visited, so that in time we may provide a better and more personalised experience for you.

You can choose whether to accept cookies by changing the settings of your browser. You can reset your browser to refuse all cookies, or allow your browser show you when a cookie is being sent. If you choose not to accept these cookies, your experience at our site may be diminished and some features may not work as intended.

Will we disclose the information you collect to outside third parties?

We may share aggregate information about our website users to third parties but will not share any personally identifiable information about you without your express consent. For example, we might inform third parties regarding the number of unique users who visit our website, the demographic breakdown of our community users of our website, or the activities that visitors to our website engage in while on our website.

We will not disclose your Personal Data to third parties unless you have consented to this disclosure or unless the third party is required to fulfil your request (in such circumstances, the need for

disclosure to a third party will have been notified to you at the time your data is collected and that third party will be bound by similar data protection requirements). We will disclose your Personal Data if we believe in good faith that we are required to disclose it in order to comply with any applicable law, a summons, a search warrant, a court or regulatory order, or other statutory requirement.

Security

Your Personal Data is held on secure servers which are hosted by us for up to 7 years. The nature of the Internet is such that we cannot guarantee or warrant the security of any information you transmit to us via the Internet. No data transmission over the Internet can be guaranteed to be 100% secure. However, we will take all reasonable steps (including appropriate technical and organisational measures) to protect your Personal Data.

Updating, verifying and deleting personal data

You may inform us of any changes in your Personal Data, and in accordance with our obligations under the Data Protection Acts 1988 and 2003, and GDPR 2018, we will update or delete your Personal Data accordingly. To find out what Personal Data we hold on you, to request a copy of your personal data or to have your Personal Data updated, amended or removed from our database, please contact us at dataprotection@paulpartnership.ie. We will respond to any data subject requests within one month of receipt of the request. No fee will be charged for this service.

Your Consent to This Agreement

By using the www.paulpartnership.ie website, you consent to the collection and use of information by us as specified above. If we decide to change our privacy policy, we will post those changes on this page so that you are always aware of what information we collect, how we use it, and under what circumstances we disclose it.

Appendix A: Employee and HR Data Retention Policy

This policy and schedule has been put in place to ensure that employee personal data is only retained for as long as is necessary for the purpose for which is was given to the organisation, and in line with both statutory requirements and individual programme funders' requirements..

1. **Job Applicants (Unsuccessful)**

Category of Personal Data	**Details**	**Retention Period**
Recruitment related data	Name, address, telephone number, email, education/ training history, employment/work history, hobbies/ interests, references, immigration status (where applicable); job specification; interview records	12 months from the date the position is filled.

2. **Job Applicants (Placed on Panel)**

Category of Personal Data	**Details**	**Retention Period**
Recruitment related data	Name, address, telephone number, email, education/ training history, employment/work history, hobbies/ interests, references, immigration status (where applicable); job specification; interview records	2 years from the date the position is filled.

3. **Employees**

Category of Personal Data	**Details**	**Retention Period**
Recruitment related data	Name, address, telephone number, email, education/ training history, employment/work history, hobbies/ interests, references, immigration status (where applicable); job specification; interview records; Garda Vetting records (where applicable)	Retained for the period of time that they are employed in the company, and for 12 months thereafter **or** for the period of time required by the relevant funding body *whichever is longer*.
Terms and conditions of employment	Personal data contained in contracts of employment, e.g., name, address, salary details;	Contracts of employment, and all related documentation to be retained for the duration of employment and for a further 7 years from the termination or expiration of the contract **or** for the period of time required by the relevant funding body *whichever is longer*.

Performance Information	Performance management review forms, notes from performance management meetings	To be retained for the duration of employment and for a further 7 years from the termination or expiration of the contract.
Grievance, disciplinary and bully & harassment investigations	Employee complaint, investigation notes, witness statements	To be retained for the duration of employment and for a further 7 years from the termination or expiration of the contract
Maternity/Adoptive leave records	Includes details regarding commencement of leave, duration of leave, notices and employee signatures	To be retained for a period of 8 years **or** for the period of time required by the relevant funding body *whichever is longer*. (There is not a minimum statutory requirement)
Parental leave/force majeure leave records	Includes details regarding commencement of leave, duration of leave, manner in which leave was taken, notices and employee signatures	As per Parental Leave Acts 1998-2006: 8 years from the date of the leave **or** for the period of time required by the relevant funding body *whichever is longer*. Notices in relation to the leave must be retained for 12 months.
Paternity leave records	Includes details regarding commencement of leave, duration of leave, manner in which leave was taken, notices and employee signatures	As per the Paternity Leave and Benefits Act 2016: 8 years from the date of leave **or** for the period of time required by the relevant funding body *whichever is longer*. Notices in relation to the leave to be retained for 12 months (not a statutory requirement).
Carer's leave records	Includes details regarding commencement of leave, duration of leave, manner in which leave was taken, notices and employee signatures	As per the Carer's Leave Act 2001: 8 years from the date of leave **or** for the period of time required by the relevant funding body *whichever is longer*. Notices in relation to the leave must be retained for 3 years.
Medical records	Includes sick leave certificates, occupational health assessments and other records relating to sick leave	To be retained for the period of time that person is employed in the company, and for 6 years thereafter **or** for the period of time required by the relevant funding body *whichever is longer*. There is no statutory retention period.
Health and Safety Records	Includes health and safety incident reports, investigation reports and other related documentation	As per the Safety, Health and Welfare at Work (General Applications) Regulations 1993: 10 years from the date of the accident/incident
Working time records	This will include details regarding weekly working hours, annual leave and public holidays, rest breaks, copy of any notices given to employee about starting and finishing times and notice of additional working hours.	As per the Organisation of Working Time Act 1997 and related Regulations: working time records must be maintained for a minimum of 3 years from the date of creation **or** for the period of time required by the relevant funding body *whichever is longer*.

Payslips	Name, salary details	As per the National Minimum Wage Act 2000: 3 years from the date of creation
Employee payroll, pension and tax records		To be retained for 7 years from the end of the financial year following termination of employment **or** to the end of any enquiry by the Revenue Commissioners **or** for the period of time required by the relevant funding body *whichever is longer*.
Employment permit records	Includes duration of employment, remuneration details, employment permit details	As per the Employment Permits Act 2003 to 2014: to be retained for a period of 5 years **or** if employed for more than 5 years - for a period equal to the duration of employment; **or** for the period of time required by the relevant funding body *whichever is longer*.
Individual Learning Plans (Labour Market Activation Programme Participants only)		To be retained for the period of time that person is employed in the company, and for 12 months thereafter.

Extension of Retention Periods

The retention periods set out above may be extended in exceptional circumstances including where records are required by the organisation to defend any legal claims taken against it or on receipt of appropriate advice.

Security of Data

The organisation will take all reasonable steps to ensure that appropriate security measures are in place to protect the confidentiality of data at all times, including during data deletion activity.

Review of Policy

The retention policy will be reviewed from time to time to take into account changes in the law and the experience of the policy in practice. The first review of the retention policy will take place after 2 years of operation.

Appendix B: IT Data Protection Security Measures

Employee Data

Recruitment

1. Specific HR email address used for recruitment access restricted to CEO and HR staff member.
2. Application forms/CVs and all other recruitment/selection documentation saved into folders, specific to every recruitment, within the HR Drive. Access to HR Drive restricted to CEO, Section Heads and HR Staff member.
3. Staff contracts saved in folders (by staff name) on HR Drive. Access restricted to CEO, Section Heads and HR Staff member.

Payroll

1. The company operate 3 payrolls – main payroll, Community Employment Childcare and Community Employment Community Outreach Team Scheme. All payrolls run on Collsoft payroll package. Access to payroll restricted to a limited number of authorised staff within Finance and within the CE Childcare and COT Teams. Each payroll is password protected.
2. The Payroll data is saved into folders on the server to which access is restricted to authorised personnel only. The data files themselves are encrypted (as part of the Collsoft software).

Client Data

Incoming Email Traffic:

1. PCs are password protected and lock after a period of time.
2. Staff are prompted to change passwords regularly.
3. Staff have dedicated email addresses – staff only have access to their own email.

Client Data Held on IT Server

1. Staff have individual private folders. Other folders are restricted to each team. Client data is saved into these folders as appropriate and access is therefore restricted to a single staff member or within a team where it is appropriate

Structural Security Measures

Our IT systems has the following security features:

- Firewalls
- Spam filter
- Anti-virus protection software
- Encryption software
- Contracted expert IT support who advise on latest issues
- Experienced in – house IT staff supported by an IT Committee

Hardware/Device Security

PCs/Desktops/mobile devices

1. No personal data is stored on the desktop of PCs
2. Laptops, mobile phones, and USB keys are encrypted and used by authorised personnel for work purposes only.

Printing/Printers

1. Printers are conveniently located in or near staff's individual offices so documents can be retrieved promptly.
2. Dedicated printers are set as a default and the printer location is visible on screen at point of printing. Staff are responsible for confirming that the printer is correct before printing and for collecting printed material from printers promptly.