

Supporting Lesbian, Gay, Bisexual &
Trans Young People in Ireland



Data Protection Policy

BeLonG To Youth Services

Table of Contents

Table of Contents	2
Revision History	4
Introduction.....	5
Scope	5
Policy Statement	5
Purpose.....	6
Penalties	6
Policy in Summary	7
The GDPR Principles.....	8
The Data Protection Team	9
Training.....	10
Lawful Basis for Processing	10
Governance Procedures.....	11
Accountability and Compliance	11
Audits and Monitoring	12
Privacy by Design	13
Data Minimisation	13
Pseudonymisation	14
Encryption	14
Restriction	15
Hard Copy Data.....	15
Records of Processing Activities.....	17
Third-Party Processors	18
Data Retention and Disposal	20
Data Protection Impact Assessments (DPIA)	20
Data Subject Rights	22
Consent Controls	23
Alternatives to Consent	24
Information Provisions	24
Privacy Policy and Notices.....	26
Privacy Notice	26
Personal Data Not Obtained from the Data Subject	27

Employee Personal Data	28
The Right of Access.....	29
Subject Access Request.....	29
Data Portability	30
Rectification and Erasure	31
Correcting Inaccurate or Incomplete Data.....	31
Right of Erasure.....	32
Right to Restrict Processing	33
Objections and Automated Decision Making	34
Oversight Procedure	35
Security and Breach Management.....	35
Passwords.....	35
Transfers and Data Sharing.....	36
Definitions	36
Information (Data) Audit	38
Appendix 1 – Related Policies.....	40

Revision History

Revision	Date of Release	Purpose
V1.0 Initial Draft	December 2014	Initial Release
V2.0	May 2018	GDPR Update
V2.1 Policy Update	January 2019	Technical Updates

Introduction

We are committed to ensuring that all personal data processed by BeLonG To Youth Services is done so in accordance with the data protection laws and its principles laid down by the Irish Data Protection Commission (National Supervisory Authority) and Irish law.

We ensure the safe, secure, ethical, and transparent processing of all personal data and have stringent measures to ensure all data subjects can exercise their data protection rights. This policy also adheres to the requirement imposed on it by the Children First Act 2015 as a mandatory reporting organisation.

Scope

This policy applies to all staff within the Organisation (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, trustees, agency workers, volunteers, interns and agents engaged with the Organisation in Ireland or overseas) and pertains to the processing of personal information. Adherence to this policy is mandatory and non-compliance could lead to serious disciplinary action.

Please refer to **Definitions** at page 36 or the Data Protection Team for any assistance required.

Policy Statement

BeLonG To Youth Services (*hereinafter referred to as the "Organisation"*) needs to collect personal information to effectively carry out our everyday organisation functions and activities and to provide the services carried out by the organisation. Such data is collected from employees, clients, service users, suppliers, funders, partners, supporters and volunteers and includes (but is not limited to), name, address, email address, data of birth, IP address, identification numbers, private and confidential information, special category (sensitive) information and bank/credit card details.

In addition, we may be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to processing all personal information in accordance with the **General Data Protection Regulation (GDPR), Irish Data Protection Laws** and any other

relevant data protection laws and codes of conduct (*herein collectively referred to as "the data protection laws"*). All reference to Articles refers to GDPR, unless otherwise stated.

The Organisation has developed policies, procedures, controls, and measures to ensure maximum and continued compliance with the data protection laws and principles, including staff training, procedure documents, audit measures and assessments. Ensuring and maintaining the security and confidentiality of personal and special category (sensitive) data is one of our top priorities and we are proud to run a **'Privacy by Design'** approach, assessing changes and their impact from the start and designing systems and processes to protect personal information at the core of our organisation.

Purpose

The purpose of this policy is to ensure that the Organisation meets its legal, statutory, and regulatory requirements under the data protection laws and to ensure that all personal and special category information is processed compliantly and, in the individuals, best interest.

The data protection laws include provisions that promote accountability and governance and as such the Organisation has put comprehensive and effective governance measures in place to meet these provisions. The aim of such measures is to minimise the risk of breaches and uphold the protection of personal data. This policy also serves as a reference document for employees, volunteers, trustees, service users, and third-parties on the responsibilities of handling and accessing personal data and data subject requests.

Penalties

The Organisation understands our obligations and responsibilities under the data protection laws and the National Supervisory Authority and we are aware of the severity of any breaches under the Regulation. We respect the National Supervisory Authority's authorisation under the legislation to impose and enforce fines and penalties on us where we breach the regulations, do not mitigate the risks where possible and operate in a knowingly non-compliant manner.

Employees have been made aware of the severity of such penalties and their proportionate nature in accordance with the breach.

Policy in Summary

The organisation has developed the below goals to meet our data protection obligations and to ensure continued compliance with the regulatory requirements.

The Organisation ensures that:

- We protect the rights of individuals with regards to the processing of personal information
- We develop, implement, and maintain a data protection policy, procedure, audit plan and training program for compliance with the data protection laws
- Every business practice, function and process carried out by the organisation, is checked for compliance with the data protection laws and its principles
- Data is only processed where we have met the lawfulness of processing requirements
- We only process special category (sensitive) data in accordance with the GDPR regulations and in compliance with the Data Protection Act requirements
- We record consent at the time it is obtained and evidence such consent to the Supervisory Authority where requested
- All employees (*including new starters, volunteers, and agents*) are competent and knowledgeable about their GDPR obligations and are provided with in-depth training in the data protection laws, principles, regulations and how they apply to their role and our organisation
- Individuals feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the data protection laws
- We have robust and documented Complaint Handling and Data Breach controls for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection
- We have appointed a **Data Protection Team** who take overall responsibility for maintaining and training and implementation of data protection for the Organisation
- We have a dedicated Audit & Monitoring Programme in place to perform regular checks and assessments on how the personal data

we process is obtained, used, stored, and shared. The audit programme is reviewed against our data protection policies, procedures, and the relevant regulations to ensure continued compliance

- We provide clear lines of reporting and supervision with regards to data protection
- We store and destroy all personal information, following the data protection laws timeframes and requirements.
- Any information provided to an individual in relation to personal data held or used about them, will be provided in a concise, transparent, intelligible, and easily accessible form, using clear and plain language
- Employees are aware of their own rights under the data protection laws and are provided with the Article 13 & 14 information disclosures
- Where applicable, we maintain records of processing activities in accordance with the Article 30 requirements
- We have developed and documented appropriate technical and organisational measures and controls for personal data security

The GDPR Principles

- a) processed lawfully, fairly and in a transparent manner in relation to the data subject (**'lawfulness, fairness and transparency'**)
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (**'purpose limitation'**)
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**'data minimisation'**)
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**'accuracy'**)
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar

as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (**'storage limitation'**)

- f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**'integrity and confidentiality'**).

Article 5(2) requires that 'the controller shall be responsible for, and be able to demonstrate, compliance with the data protection laws principles' (**'accountability'**) and requires that firms **show how** they comply with the principles, detailing and summarising the measures and controls that they have in place to protect personal information and mitigate the risks of processing.

The Data Protection Team

The Organisation has appointed a Data Protection Team their role is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the organisation, its employees, volunteers, trustees, and senior leadership and to actively stay informed and up-to-date with all legislation and changes relating to data protection.

The Data Protection Team will work in conjunction with relevant department heads to ensure that all processes, systems and staff/ volunteers are operating compliantly and within the requirements of the data protection laws and its principles.

The Data Protection Team has overall responsibility for due diligence, privacy impact assessments, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the data protection laws and our own internal objectives and obligations.

Staff who manage and process personal or special category information will be provided with extensive data protection training and will be subject to continuous development support and mentoring to ensure that they are competent and knowledgeable for the role they undertake.

The Data Protection Team is:

Oisín O'Reilly Head of Fundraising and Operations
Suzanne Handley Finance Manager

They can be contacted by emailing privacy@belongto.org

Training

Through our strong commitment and robust controls, we ensure that all staff understand, have access to and can easily interpret the data protection laws requirements and its Principles and that they have ongoing training, support, and assessments to ensure and demonstrate their knowledge, competence and adequacy for the role. Our **Training & Development Policy & Procedures** and **Induction Policy** detail how new and existing employees are trained, assessed, and supported and include: -

- GDPR Workshops & Training Sessions
- Assessment Tests
- Coaching & Mentoring
- 1:1 Support Sessions
- Scripts and Reminder Aids
- Access to GDPR policies, procedures, checklists and supporting documents

Employees are continually supported and trained in the data protection laws requirements and out own objectives and obligations around data protection.

Lawful Basis for Processing

At the core of all personal information processing activities undertaken by the Organisation, is the assurance and verification that we are following

Article 6 of the data protection laws and our lawfulness of processing obligations. Prior to carrying out any processing activity on personal information, we always identify and establish the legal basis for doing so and verify these with the regulations.

This legal basis is documented on our information audit register and where applicable, is provided to the data subject and Supervisory Authority.

Data is only obtained, processed, or stored when we have met the lawfulness of processing requirements, where:

- The data subject has given **consent** to the processing of their personal data for one or more specific purposes
- Processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a **legal obligation** to which we are subject
- Processing is necessary in order to **protect the vital interests** of the data subject or of another natural person
- Processing is necessary for the performance of a task carried out **in the public interest** or in the exercise of official authority vested in the Organisation
- Processing is necessary for the purposes of the **legitimate interests** pursued by the Organisation or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child).

Governance Procedures

Accountability and Compliance

Due to the nature, scope, context, and purposes of processing undertaken by the Organisation, we carry out frequent risk assessments and information audits to identify, assess, measure and monitor the impact of such processing.

We have also implemented adequate and appropriate technical and organisational measures to ensure the safeguarding of personal data and compliance with the data protection laws.

We can demonstrate that all processing activities are performed in accordance with the data protection laws and that we have in place robust policies, procedures, measures and controls for the protection of data.

Our main governance objectives are to:

- Educate senior management and employees about the requirements under the data protection laws and the possible impact of non-compliance
- Provide a dedicated and effective data protection training program for all staff
- Identify key senior stakeholders to support the data protection compliance program
- Allocate responsibility for data protection compliance and ensure that the designated team has sufficient access, support and budget to perform the role
- Identify, create and disseminate the reporting lines within the data protection governance structure

The technical and organisational measures that the Organisation has in place to ensure and demonstrate compliance with the data protection laws, regulations and codes of conduct, are detailed in this document and associated policies.

Audits and Monitoring

This policy and procedure document details the extensive controls, measures and methods used by the Organisation to protect personal data, uphold the rights of data subjects, mitigate risks, minimise breaches and comply with the data protection laws and associated laws and codes of conduct.

The Data Protection Team has overall responsibility for assessing, testing, reviewing and improving the processes, measures and controls in place and reporting improvement action plans to the Senior Management Team where applicable. Data minimisation methods are frequently reviewed, and new technologies assessed to ensure that we are protecting data and individuals to the best of our ability.

All reviews, audits and ongoing monitoring processes are recorded by the Data Protection Team and copies provided to Senior Management and are made readily available to the Supervisory Authority where requested.

Privacy by Design

We operate a 'privacy by design' approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via our processes, systems and activities. We therefore have added measures in place to adhere to this ethos, including:

Data Minimisation

Data should be '*limited to what is necessary*', which forms the basis of our minimal approach. We only ever obtain, retain, process and share the data that is essential to carry out our services and legal obligations and we only keep it for as long as is necessary.

Our systems, employees, processes, and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to carry out the specified purpose. Data minimisation enables us to reduce data protection risks and breaches and supports our compliance with the data protection laws.

Measures to ensure that only the necessary data is collected include: -

- Electronic collection (*i.e. forms, website, surveys etc*) only have the fields that are relevant to the purpose of collection and subsequent processing. We do not include 'optional' fields, as optional denotes that it is not necessary to obtain
- Physical collection (*i.e. face-to-face, telephone etc*) is supported using scripts and internal forms where the required data collection is ascertained using predefined fields. Again, only that which is relevant and necessary is collected
- We have SLA's and bespoke agreements in place with third-party controllers who send us personal information (*either in our capacity as a controller or processor*). These state that only relevant and necessary data is to be provided as it relates to the processing activity we are carrying out.

- We have documented destruction procedures in place where a data subject or third-party provides us with personal information that is surplus to requirement.

Pseudonymisation

With regard to hard copy files, we utilise pseudonymisation where possible to record and store personal data in a way that ensures data can no longer be attributed to a specific data subject without the use of separate additional information (personal identifiers). Encryption and partitioning is also used to protect the personal identifiers, which are always kept separate from the pseudonymised data sets.

When using pseudonymisation, we ensure that the attribute(s) being removed and replaced, are unique and prevent the data subject from being identified through the remaining markers and attributes. Pseudonymisation means that the data subject is still likely to be identified indirectly and as such, we use this technique in conjunction with other technical and operational measures of risk reduction and data protection.

When Storing data electronically, data subjects are offered the opportunity to store their data under a pseudonym. However, if they wish to store their data under their own name we will follow this request meaning each person has a profile assigned to their name containing their personal data. We have procedures which do not allow staff export data from the database which includes a person's name.

Encryption

Although we class encryption as a form of pseudonymisation, we also utilise it as a secondary risk prevention measure for securing the personal data that we hold. Encryption with a secret key is used to make data indecipherable unless decryption of the dataset is carried out using the assigned key.

We utilise encryption via secret key for transferring personal data to any external party and provide the secret key in a separate format. Where special category information is being transferred and/or disclosed, the Data Protection Team is required to authorise the transfer and review the encryption method for compliance and accuracy.

All devices (mobiles, computers, laptops) connected to the organisations networks and systems used for storing personal information are required

to be encrypted prior to the device being granted access to the data. Personal information contained within databases and in file servers is encrypted at rest within at least two secure data centres located within the EU.

Restriction

Our *Privacy by Design* approach means that we use Organisation-wide restriction methods for all personal data activities. Restricting access is built into the foundation of the Organisation's processes, systems and structure and ensures that only those with authorisation and/or a relevant purpose, have access to personal information. Special category data is restricted at all levels and can only be accessed on a need to know basis.

Hard Copy Data

Due to the nature of our organisation, it is sometimes essential for us to obtain, process and share personal and special category information which is only available in a paper format without pseudonymisation options (e.g. Staff Notebooks). Where this is necessary, we utilise a tiered approach to minimise the information we hold and/or the length of time in which we hold it.

Steps include:

- In the first instance, we always ask the initial data controller to send copies of any personal information records directly to the data subject
- Where step 1 is not possible or workable, we will obtain a copy of the data and if applicable redact to ensure that only the relevant information remains (i.e. when the data is being passed to a third-party for processing and not directly to the data subject)
- When only mandatory information is visible on the hard copy data, we utilise electronic formats to send the information to the recipient to ensure that encryption methods can be applied (i.e. we do not use the postal system as this can be intercepted)
- Recipients (i.e. the data subject, third-party processor) are reverified and their identity and contact details checked.
- The Data Protection Team authorises the transfer and checks the file(s) attached and encryption method and key
- Once confirmation has been obtained that the recipient has received the

personal information, where possible (within the legal guidelines and rules of the data protection laws), we destroy the hard copy data and delete the sent message

- If for any reason a copy of the paper data must be retained by the Organisation, we use a physical safe to store such documents as oppose to our standard archiving system

Special categories of Personal Data are defined in the data protection laws as:

- a) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies.
- b) Where the Organisation processes any personal information classed as special category data or information relating to criminal convictions, we do so in accordance with the data protection laws Article 9 regulations and in compliance with the Data Protection Act 2018 requirements.

We will only ever process special category data where: -

- The data subject has given explicit consent to the processing of the personal
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim
- Processing relates to personal data which are manifestly made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity

- Processing is necessary for reasons of substantial public interest
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
- Processing is necessary for reasons of public interest in the area of public health
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)

The Data Protection Act 2018 provides specific conditions and circumstances when special category personal data can be processed and dictated the requirements that organisations are obligated to meet when processing such data.

Where the Organisation processes personal data that falls into one of the above categories, we have the specified provisions and measures in place prior to any processing.

Measures include:

- Verifying our reliance on one of the data protection laws Article 9(1), and where applicable conditions under The Data Protection Act 2018 prior to processing
- Having an appropriate policy document in place when the processing is carried out, specifying our: -
 - procedures for securing compliance with the data protection laws principles
 - policies as regards the retention and erasure of personal data processed in reliance on the condition
 - retention periods and reason (*i.e. legal, statutory etc*)
 - procedures for reviewing and updating our policies in this area

Please refer to our Retention and Erasure Policy for further guidance and procedures.

Records of Processing Activities

As an organisation with less than 250 employees, the Organisation maintains records of all processing activities where: -

- Processing personal data could result in a risk to the rights and freedoms of individual
- The processing is not occasional
- We process special categories of data or criminal convictions and offences
- Such records are maintained in writing, are provided in a clear and easy to read format and are readily available to the Supervisory Authority upon request.

Third-Party Processors

The Organisation utilise external processors for certain processing activities (where applicable). We use information audits to identify, categorise and record all personal data that is processed outside of the Organisation, so that the information, processing activity, processor and legal basis are all recorded, reviewed and easily accessible. Such external processing includes (but is not limited to):

- IT Systems and Services
- Legal Services
- Human Resources
- Finance, Payroll, and Accounting Services
- Direct Marketing Services

We have strict due diligence and Know Your Customer procedures and measures in place and review, assess and background check all processors prior to forming a business relationship. We obtain Organisation documents, certifications, references and ensure that the processor is adequate, appropriate and effective for the task we are employing them for.

We audit their processes and activities prior to contract and during the contract period to ensure compliance with the data protection regulations

and review any codes of conduct that they are obligated under to confirm compliance. The continued protection of the rights of the data subjects is our priority when choosing a processor and we understand the importance of outsourcing processing activities as well as our continued obligations under the data protection laws even when a process is handled by a third-party.

We have Service Level Agreements (SLAs) and contracts with each processor and among other details, outlines the following:

- The processors data protection obligations
- Our expectations, rights, and obligations
- The processing duration aims and objectives
- The data subjects' rights and safeguarding measures
- The nature and purpose of the processing
- The type of personal data and categories of data subjects

Each of the areas specified in the contract are monitored, audited and reported on. Processors are notified that they shall not engage another processor without our prior specific authorisation and any intended changes concerning the addition or replacement of existing processors must be done in writing, in advance of any such changes being implemented.

That contract or other legal act shall stipulate, in particular, that the processor:

- Processes the personal data only on our documented instructions
- Seeks our authorisation to transfer personal data to a third country or an international organisation (unless required to do so by a law to which the processor is subject)
- Shall inform us of any such legal requirement to transfer data before processing
- Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
- Takes all measures to security the personal data at all times
- Respects, supports, and complies with our obligation to respond to requests for exercising the data subject's rights
- Assists the Organisation in ensuring compliance with our obligations for data security, mitigating risks, breach notification and privacy impact assessments

- When requested, deletes or returns all personal data to the Organisation after the end of the provision of services relating to processing, and deletes existing copies where possible
- Makes available to the Organisation, all information necessary to demonstrate compliance with the obligations set out here and, in the contract
- Allows and supports audits, monitoring, inspections, and reporting as set out in the contract

Informs the Organisation immediately of any breaches, non-compliance or inability to carry out their duties as detailed in the contract.

Data Retention and Disposal

The Organisation have defined procedures for adhering to the retention periods as set out by the relevant laws, contracts, and business requirements, as well as adhering to the data protection laws requirement to only hold and process personal information for as long as is necessary.

All personal data is disposed of in a way that protects the rights and privacy of data subjects (*e.g. shredding, disposal as confidential waste, secure electronic deletion*) and always prioritises the protection of the personal data.

Please refer to our **Data Retention & Erasure Policy** for full details on our retention, storage, periods, and destruction processes.

Data Protection Impact Assessments (DPIA)

Individuals have an expectation that their privacy and confidentiality will be upheld and respected whilst their data is being stored and processed by the Organisation. We therefore utilise several measures and tools to reduce risks and breaches for general processing, however when the processing is likely to be elevated risk or cause significant impact to a data subject, we utilise proportionate methods to map out and assess the impact ahead of time.

Where the Organisation must or are considering carrying out processing that utilises new technologies, and/or where there is a likelihood that such processing could result in a high risk to the rights and freedoms of data subjects, we always carry out a Data Protection Impact Assessment (DPIA) (*sometimes referred to as a Privacy Impact Assessment*).

Pursuant to Article 35(3) and Recitals 84, 89-96, we consider processing that is likely to result in a high risk to include: -

- Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person(s)
- Processing on a large scale of special categories of data
- Processing on a large scale of personal data relating to criminal convictions and offences
- Systematic monitoring of a publicly accessible area on a large scale (i.e. CCTV)
- Where a processing operation is likely to result in a high risk to the rights and freedoms of an individual
- Those involving the use of new technologies
- New processing activities not previously used
- Processing considerable amounts of personal data at regional, national, or supranational level, which could affect many data subjects
- Processing activities making it difficult for the data subject(s) to exercise their rights

Carrying out DPIAs enables us to identify the most effective way to comply with our data protection obligations and ensure the highest level of data privacy when processing. It is part of our Privacy by Design approach and allows us to assess the impact and risk before carrying out the processing, thus identifying and correcting issues at the source, reducing costs, breaches, and risks.

The DPIA enables us to identify possible privacy solutions and mitigating actions to address the risks and reduce the impact. Solutions and suggestions are set out in the DPIA and all risks are rated to assess their likelihood and impact. The aim of solutions and mitigating actions for all risks is to ensure that the risk is either: -

- Eliminated
- Reduced
- Accepted

For further information please see our DPIA procedures.

Data Subject Rights

The collection of personal and sometimes special category data is a fundamental part of the services offered by the Organisation and we therefore have specific measures and controls in place to ensure that we comply with the conditions for consent under the data protection laws.

The data protection laws define consent as; 'Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.

Consent requests are transparent, using plain language and is void of any illegible terms, jargon or extensive legal terms:

- It is freely given, specific and informed, as well as being an unambiguous indication of the individual's wishes
- Consent is always given by a statement or a clear affirmative action (positive opt-in) which signifies agreement to the processing of personal data
- Consent mechanisms are upfront, clear, granular (in fine detail) and easy to use and understand
- Pre-ticked, opt-in boxes are never used
- Where consent is given as part of other matters (i.e. terms & conditions, agreements, contracts), we ensure that the consent is separate from the other matters and is not be a precondition of any service (unless necessary for that service)
- Along with our Organisation name, we also provide details of any other third party who will use or rely on the consent
- Consent is always verifiable, and we have controls in place to ensure that we can demonstrate consent in every case
- We keep detailed records of consent and can evidence at a minimum:
 - that the individual has consented to the use and processing of their personal data
 - that the individual has been advised of our Organisation name and any third party using the data
 - what the individual was told at the time of consent

- how and when consent was obtained
- We have ensured that withdrawing consent is as easy, clear, and straightforward as giving it and is available through multiple options, including:
 - Opt-out links in mailings or electronic communications
 - Opt-out process explanation and steps on website and in all written communications
 - Ability to opt-out verbally, in writing or by email or over the phone
- Consent withdrawal requests are processed immediately and without detriment
- Controls and processes have been developed and implemented to refresh consent, especially those relating to parental consents
- For special category data, the consent obtained is explicit (stated clearly and in detail, leaving no room for confusion or doubt) with the processing purpose(s) always being specified

Consent Controls

The Organisation maintain rigid records of data subject consent for processing personal data and are always able to demonstrate that the data subject has consented to processing of his or her personal data where applicable. We also ensure that the withdrawal of consent is as clear, simple and transparent as it is to give consent.

Where the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent is presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. All such written declarations are reviewed and authorised by the Data Protection Team prior to being circulated.

Consent to obtain, process, store, and share (*where applicable*), is obtained by the organisation through:

- Face-to-Face
- Telephone
- In Writing

- Email/SMS
- Electronic (i.e. via website form)

Points 1-4 are enforced using scripts, checklists, on-screen prompts, and signed customer agreements, to ensure that consent has been obtained and to remind employees of their added consent obligations, as below.

Electronic consent is always by a non-ticked, opt-in action (*or double opt-in where applicable*), enabling the individual to provide consent after the below information has been provided. This is then followed up with an email, SMS, or written confirmation of the consent to process, store and share the personal information.

Privacy Notices are used in all forms of consent and personal data collection, to ensure that we are compliant in disclosing the information required in the data protection laws in an easy to read and accessible format.

Alternatives to Consent

The Organisation recognise that there are six lawful bases for processing and that consent is not always the most appropriate option. We have reviewed all processing activities and only use consent as an option where the individual has a choice.

Information Provisions

Where personal data is obtained directly from the individual (*i.e. through consent, by staff or volunteers, written materials, and/or electronic formats (i.e. website forms, subscriptions, email etc)*), we provide the below information in all instances, in the form of a consent/privacy notice:

- The identity and the contact details of the controller and, where applicable, of the controller's representative
- The contact details of our Data Protection Team
- The purpose(s) of the processing for which the personal information is intended
- The legal basis for the processing
- Where the processing is based on point (f) of Article 6(1) "processing is necessary for the purposes of the legitimate interests

pursued by the controller or by a third party", details of the legitimate interests

- The recipients or categories of recipients of the personal data (if applicable)
- If applicable, the fact that the Organisation intends to transfer the personal data to a third country or international organisation and the existence/absence of an adequacy decision by the European Commission
 - where the Organisation intends to transfer the personal data to a third country or international organisation without an adequate decision by the European Commission, reference to the appropriate or suitable safeguards the Organisation has put into place and the means by which to obtain a copy of them or where they have been made available
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- The existence of the right to request access to and rectification or erasure of, personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
- Where the processing is based on consent under points (a) of Article 6(1) or Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- The right to lodge a complaint with the Supervisory Authority
- Whether providing personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data
- The existence of any automated decision-making, including profiling, as referred to in Article 22(1) and (4) and explanatory information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject
 - The above information is provided to the data subject at the time the information is collected and records pertaining to the consent obtained are maintained and stored for 6 years from

the date of consent, unless there is a legal requirement to keep the information longer.

Privacy Policy and Notices

The Organisation recognises the difference between a Privacy Policy and a Privacy Notice (or statement) and ensures that we meet the regulatory, legal, and best practice requirements for both formats. For the purposes of this document, we use the term Privacy Policy to provide the business, its staff, volunteers, trustees and any associated entities with our operational and organisational approach to protecting data and complying with the General Data Protection Regulation (GDPR) and the relevant the data protection laws.

This document is our Data Protection Policy and includes how we comply with the data protection laws principles, the manner in which we process data, guidelines and procedures for ensuring that data subjects can exercise their rights and our approach to data protection by design and default. This policy provides detail on how we apply the principles, what procedures we follow in the compliance with the Regulation and any specific individual and/or departmental responsibilities, including those of the Data Protection Team and is fundamentally used as an internal reference document.

We have a user-friendly version on our website, which also includes details about the cookies used on the site. The Privacy Notice on the site is in an easy to see and accessible place and is in addition to our legally required Privacy Notice; more details of which are noted below.

Privacy Notice

Our Privacy Notice is separate from our Data Protection Policy and is provided to individuals at the time we collect their personal data (or at the earliest possibility where that data is obtained indirectly). Our Privacy Notice includes the Article 13 & 14 (*section 21 of this policy*) requirements as set out in the data protection laws and provides individuals with all the necessary and legal information about how, why and when we process their data, along with their rights and obligations.

Our Privacy Notice is designed to be a public declaration of how the Organisation applies the data protection principles to data that we process. It is provided to all individuals whose data we process (i.e.

service users, employees, third-parties etc) and contains only the information specific to the individual and as required by law. The notice is easily accessible, legible, jargon-free and is available in several formats, dependant on the method of data collection:

- Via our website
- Linked to or written in full in the footer of emails
- Worded in full in agreements, contracts, forms, and other materials where data is collected in writing or face-to-face
- In employee contracts and recruitment materials
- Verbally via telephone or face-to-face
- Printed media, adverts, and promotions
- Digital Products/Services

With lengthy content being provided in the privacy notice and with informed consent being based on its contents, we have tested, assessed, and reviewed our privacy notice to ensure usability, effectiveness and understanding.

Where we rely on consent to obtain and process personal information, we ensure that it is:

- Displayed clearly and prominently
- Asks individuals to positively opt-in
- Gives them sufficient information to make an informed choice
- Explains the different ways we will use their information
- Provides a clear and simple way for them to indicate they agree to different types of processing
- Includes a separate unticked opt-in box for direct marketing/fundraising communications

Personal Data Not Obtained from the Data Subject

Where the Organisation obtains and/or processes personal data that has **not** been obtained directly from the data subject, the Organisation ensures that the information noted in 'Privacy Policy and Notices Section' (page 26) of this policy is provided to the data subject within 30 days of

our obtaining the personal data (*except for advising if the personal data is a statutory or contractual requirement*).

In addition to the information provided to the data subject section of this policy, we also provide information about:

- The categories of personal data
- The source the personal data originated from and whether it came from publicly accessible sources

Where the personal data is to be used for communication with the data subject, or a disclosure to another recipient is envisaged, the information will be provided at the latest, at the time of the first communication or disclosure. Where the Organisation intends to further process any personal data for a purpose **other** than that for which it was originally obtained, we communicate this intention to the data subject prior doing so and where applicable, process only with their consent.

Whilst we follow best practice in the provision of the information noted in the relevant section of this policy, we reserve the right not to provide the data subject with the information if:

- They already have it and we can evidence their prior receipt of the information
- The provision of such information proves impossible and/or would involve a disproportionate effort
- Obtaining or disclosure is expressly laid down by Union or Member State law to which the Organisation is subject and which provides appropriate measures to protect the data subject's legitimate interest
- Where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy

Employee Personal Data

As per the data protection laws guidelines, we do not use consent as a legal basis for obtaining or processing necessary employee personal information. We provide our employees with an Employee Privacy Notice to ensure that employees are provided with the appropriate information disclosure and are aware of how we process their data and why.

All employees are provided with our Staff Handbook which informs them of their rights under the data protection laws and how to exercise these rights.

The Right of Access

We have ensured that appropriate measures have been taken to provide information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 (collectively, The Rights of Data Subjects), relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Such information is provided free of charge and is in writing, or by other means where authorised by the data subject and with prior verification as to the subject's identity (*i.e. verbally, electronic*).

Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request is received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.

Where we do not comply with a request for data provision, the data subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority.

Subject Access Request

Where a data subject asks us to confirm whether we hold and process personal data concerning him or her and requests access to such data; we provide them with: -

- The purposes of the processing
- The categories of personal data concerned
- The recipients or categories of recipient to whom the personal data have been or will be disclosed

- If the data has or will be disclosed to a third countries or international organisations and the appropriate safeguards pursuant to the transfer
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- The right to lodge a complaint with a Supervisory Authority
- Where personal data has not been collected by the Organisation from the data subject, any available information as to the source and provider
- The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

Subject Access Requests (SAR) are passed to the Data Protection Team as soon as received and a record of the request is noted. The type of personal data held about the individual is checked against our Information Audit to see what format it is held in, who else has it has been shared with and any specific timeframes for access.

SARs are always completed within 30-days and are provided free of charge. Where the individual makes the request by electronic means, we provide the information in a commonly used electronic format, unless an alternative format is requested, and it is technically possible with reasonable effort.

Please refer to our external Subject Access Request Procedures for the guidelines on how an SAR can be made and what steps we take to ensure that access is provided under the data protection laws.

Data Portability

The Organisation provides all personal information pertaining to the data subject to them on request and in a format, that is easy to disclose and read. We ensure that we comply with the data portability rights of

individuals by ensuring that all personal data is readily available and is in a structured, commonly used and machine-readable format, enabling data subjects to obtain and reuse their personal data for their own purposes across different services.

To ensure that we comply with Article 20 of the GDPR concerning data portability, we keep a commonly used and machine-readable format of personal information where the processing is based on: -

- Consent pursuant to point (a) of Article 6(1)
- Consent pursuant to point (a) of Article 9(2)
- A contract pursuant to point (b) of Article 6(1); and
- the processing is carried out by automated means

Where requested by a data subject and if the criteria meet the above conditions, we will transmit the personal data directly from the Organisation to a designated controller, where technically feasible.

We utilise the below formats for the machine-readable data: -

- CSV

All requests for information to be provided to the data subject or a designated controller are done so free of charge and within 30 days of the request being received. If for any reason, we do not act in responding to a request, we provide a full, written explanation within 30 days to the data subject or the reasons for refusal and of their right to complain to the supervisory authority and to a judicial remedy.

All transmission requests under the portability right are assessed to ensure that no other data subject is concerned. Where the personal data relates to more individuals than the subject requesting the data/transmission to another controller, this is always without prejudice to the rights and freedoms of the other data subjects.

Rectification and Erasure

Correcting Inaccurate or Incomplete Data

- Pursuant to Article 5(d), all data held and processed by the Organisation is reviewed and verified as being accurate wherever possible and is always kept up to date. Where inconsistencies are identified and/or where the data subject or controller inform us that the data, we hold is inaccurate, we take every reasonable

step to ensure that such inaccuracies are corrected with immediate effect.

- The Data Protection Team are notified of the data subjects request to update personal data and are responsible for validating the information and rectifying errors where they have been notified. The information is altered as directed by the data subject, with the information audit being checked to ensure that all data relating to the subject is updated where incomplete or inaccurate. Once updated, we add an addendum or supplementary statement where applicable.
- Notified of inaccurate data by the data subject, we will rectify the error within 30 days and inform any third party of the rectification if we have disclosed the personal data in question to them. The data subject is informed in writing of the correction and where applicable, is provided with the details of any third-party to whom the data has been disclosed.
- If for any reason, we are unable to act in response to a request for rectification and/or completion, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

Right of Erasure

- Also, known as '*The Right to be Forgotten*', the Organisation complies fully with Article 5(e) and ensures that personal data which identifies a data subject, is not kept longer than is necessary for the purposes for which the personal data is processed.
- All personal data obtained and processed by the Organisation is categorised when assessed by the information audit and is either given an erasure date or is monitored so that it can be destroyed when no longer necessary.
- Please refer to our Data Retention & Erasure Policy for exact procedures on erasing data and complying with the Article 17 requirements

Right to Restrict Processing

There are certain circumstances where the Organisation restricts the processing of personal information, to validate, verify or comply with a legal requirement of a data subject's request. Restricted data is removed from the normal flow of information and is recorded as being restricted on the information audit.

Any account and/or system related to the data subject of restricted data is updated to notify users of the restriction category and reason. When data is restricted it is only stored and not processed in any way.

The Organisation will apply restrictions to data processing in the following circumstances:

- Where an individual contests the accuracy of the personal data and we are in the process verifying the accuracy of the personal data and/or making corrections
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether we have legitimate grounds to override those of the individual
- When processing is deemed to have been unlawful, but the data subject requests restriction as oppose to erasure
- Where we no longer need the personal data, but the data subject requires the data to establish, exercise or defend a legal claim

The Data Protection Team reviews and authorises all restriction requests and actions and retains copies of notifications from and to data subjects and relevant third-parties. Where data is restricted, and we have disclosed such data to a third-party, we will inform the third-party of the restriction in place and the reason and re-inform them if any such restriction is lifted.

Data subjects who have requested restriction of data are informed within 30 days of the restriction application and are also advised of any third-party to whom the data has been disclosed. We also provide in writing to the data subject, any decision to lift a restriction on processing. If for any reason, we are unable to act in response to a request for restriction, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

Objections and Automated Decision Making

- Data subjects are informed of their right to object to processing in our Privacy Notices and at the point of first communication, in a clear and legible form and separate from other information. We provide opt-out options on all direct marketing material and provide an online objection form where processing is carried out online.

Individuals have the right to object to:

- Processing of their personal information based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- Direct marketing (including profiling)
- Processing for purposes of scientific/historical research and statistics
- Where the Organisation processes personal data for the performance of a legal task, in relation to our legitimate interests or for research purposes, a data subjects' objection will only be considered where it is on '*grounds relating to their particular situation*'. We reserve the right to continue processing such personal data where: -
 - We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
 - The processing is for the establishment, exercise or defence of legal claims
- Where we are processing personal information for direct marketing purposes under a previously obtained consent, we will stop processing such personal data immediately where an objection is received from the data subject. This measure is absolute, free of charge and is always adhered to.
- Where a data subject objects to data processing on valid grounds, the organisation will cease the processing for that purpose and advise the data subject of cessation in writing within 30 days of the objection being received.

Oversight Procedure

Security and Breach Management

Alongside our *'Privacy by Design'* approach to protecting data, we ensure the maximum security of data that is processed, including as a priority, when it is shared, disclosed and transferred. Our **Information Security Policy and Procedures** provide the detailed measures and controls that we take to protect personal information and to ensure its security from consent to disposal.

We carry out information audits to ensure that all personal data held and processed by us is accounted for and recorded, alongside risk assessments as to the scope and affect a data breach could have on data subject(s). We have implemented adequate and appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Whilst every effort and measure are taken to reduce the risk of data breaches, the Organisation has dedicated controls and procedures in place for such situations, along with the notifications to be made to the Supervisory Authority and data subjects (where applicable).

Please refer to our **Data Breach Policy and Procedures** for specific protocols.

Passwords

Passwords are a key part of the Organisation protection strategy and are used throughout the Organisation to secure information and restrict access to systems. We use a multi-tiered approach which includes passwords at user, management, device, system, and network levels to ensure a thorough and encompassing approach.

Whilst passwords are also directly related to Information Security and Access Control, the Organisation recognises that strong, effective and robust password controls and measures are imperative to the protection and security of personal information.

Passwords afford a high level of protection to resources and data and are mandatory requirements for all employees and/or third-parties who are responsible for one or more account, system or have access to any resource that requires a password. Full procedures and guidelines for passwords, access and security can be found in our **Information Security Policy and Procedures**.

Transfers and Data Sharing

The Organisation takes proportionate and effective measures to protect personal data held and processed by us at all times, however we recognise the high-risk nature of disclosing and transferring personal data and as such, place an even higher priority on the protection and security of data being transferred. Data transfers within Ireland and EU are deemed less of a risk than a third country or an international organisation, due to the data protection laws covering the former and the strict regulations applicable to all EU Member States.

Where data is being transferred for a legal and necessary purpose, compliant with all Articles in the Regulation, we utilise a processes that ensures appropriate security and where possible is also subject to our data minimisation methods. We use approved, secure methods of transfer and have dedicated points of contact with each Member State organisation with whom we deal. All data being transferred is noted on our information audit so that tracking is easily available, and authorisation is accessible. The Data Protection Team authorises all EU transfers and verifies the encryption and security methods and measures.

All organisations in third countries to whom we transfer data will be fully compliant with the requirements of GDPR and will be required to have incorporated the 'standard contractual clauses' approved by the European Commission or by the Supervisory Authority or have adopted 'binding corporate rules' as appropriate.

Definitions

- **"Article or recital [no]"** refers to an article or recital of the General Data Protection Regulation (EU) (2016/679).
- **"Biometric data"** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
- **"Binding Corporate Rules"** means personal data protection policies which are adhered to by the Organisation for transfers of

personal data to a controller or processor in one or more third countries or to an international organisation.

- **"Consent"** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- **"Cross Border Processing"** means processing of personal data which: -
 - takes place in more than one Member State; or
 - which substantially affects or is likely to affect data subjects in more than one Member State
- **"Data controller"** means, the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- **"Data processor"** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- **"Data protection laws"** means for the purposes of this document, the collective description of the GDPR, Data Protection Act 2018 and any other relevant data protection laws that the Organisation complies with.
- **"Data subject"** means an individual who is the subject of personal data
- **"GDPR"** means the General Data Protection Regulation (EU) (2016/679)
- **"Genetic data"** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
- **"Personal data"** means any information relating to an identified or identifiable natural person (*'data subject'*); an identifiable natural person is one who can be identified, directly or indirectly, in particular

by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- **"Processing"** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **"Profiling"** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- **"Recipient"** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
- **"Supervisory Authority"** means the Irish Data Protection Commission
- **"Third Party"** means a natural or legal person, public authority, agency or body other than the data subject, under our direct authority

Information (Data) Audit

To enable the Organisation to fully prepare for and comply with the data protection laws, we have carried out an organisation-wide data protection information audit to better enable us to record, categorise and protect the personal data that we hold and process. Audit data is securely stored and available to the Supervisory Authority to inspect.

The audit has identified, categorised and recorded all personal information obtained, processed and shared by our Organisation in our capacity as a controller/processor and has been compiled on a central register which includes: -

- What personal data we hold
- Where it came from
- Who we share it with
- Legal basis for processing it
- What format(s) is it in
- Who is responsible for it?
- Disclosures and Transfers

Appendix 1 – Related Policies

1. Data Retention and Erasure Policy
2. Data Processor Agreement
3. Privacy Notice
4. Employee and Volunteer Privacy Notice
5. Feedback, Compliments and Complaints Policy
6. Subject Access Request Procedures
7. Data Breach Policy
8. Data Protection Impact Assessment Procedure
9. Internal Audit and Monitoring Policy
10. Information Security Policy
11. Training and Development Policy
12. Safeguarding and Child Protection Policy