	Gasóga na hÉireann / Scouting Ireland			
	No.	Issued	Amended	Next Review Date
	SI-DP01	20.08.2021	n/a	20.08.2022
	Category: Data Protection			
	Scouting Ireland - Data Protection Policy			

Related Documents

Revision Schedule			
Version	***Revision Date***	***Revised by***	***Section Revised***

Document Control

Document Owner:	***Document No:***	***Status:***	***Date Approved:***
ICD	SI-DP01	Approved	15.08.2021
Security Classification:	***Next Review Date:***	***Version: 1.0***	***Department:***
High/Medium/Low	20.08.2022		ICD

Data Protection Policy

Contents

1 POLICY STATEMENT

Scouting Ireland needs to collect personal information to effectively carry out our everyday business functions and activities and to provide the products and services defined by our business type. Such data is collected from employees, customers, suppliers and clients and includes *(but is not limited to),* name, address, email address, data of birth, phone numbers, identification numbers, private and confidential information, 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 the data protection laws and codes of conduct *(herein collectively referred to as **"the data protection laws"**).*

Scouting Ireland 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/or special category data is one of our top priorities and we are proud to operate a ***'Privacy by Design'*** approach, assessing changes and their impact from the start and designing systems and processes to protect personal information.

2 PURPOSE

The purpose of this policy is to ensure that Scouting Ireland 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 best interest of the individual.

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

3 SCOPE

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

3.1 GENERAL DATA PROTECTION REGULATION (GDPR)

The ***General Data Protection Regulation (GDPR) (EU) 2016/679)*** was approved by the European Commission in April 2016 and will apply to all EU Member States from 25th May 2018. As a

'Regulation' rather than a *'Directive'*, its rules apply directly to Member States, replacing their existing local data protection laws and repealing and replacing Directive 95/46EC and its Member State implementing legislation. So also (for scouts in NI) does the UK Data Protection Bill 2018.

As Scouting Ireland processes personal information regarding individuals (*data subjects*), we are obligated under the General Data Protection Regulation (GDPR) and the UK Data Protection Bill 2018 (for scouts in NI) to protect such information, and to obtain, use, process, store and destroy it, only in compliance with its rules and principles.

3.1.1 PERSONAL DATA

Information protected under the GDPR is known as *"personal data"* and is defined as: -

"Any information relating to an identified or identifiable natural person; 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."

Scouting Ireland ensures that a high level of care is afforded to personal data falling within the GDPR's **'special categories'** *(previously **sensitive personal data***), due to the assumption that this type of information could be used in a negative or discriminatory way and is of a sensitive, personal nature to the persons it relates to.

In relation to the 'Special categories of Personal Data' the GDPR advises that: -

"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."

3.1.2 THE GDPR PRINCIPLES

Article 5 of the GDPR requires that personal data shall be: -

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.

3.2 THE OFFICE OF THE DATA PROTECTION COMMISSIONER (DPC)

The DPC is an independent regulatory office whose role it is to uphold information rights in the public interest. The legislation they have oversight for includes: -

- The Data Protection Acts 1988 and 2003 *(pre-25th May 2018)*
- General Data Protection Regulation *(post-25th May 2018)*
- The Privacy and Electronic Communication (EU Directive) Regulations 2011

The DPC's mission statement is *"to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals"* and they can issue enforcement notices and fines for breaches under any of the Regulations, Acts and/or Laws regulated by them.

Under the data protection laws the DPC, as Ireland's data protection authority (*Supervisory Authority*), will have a similar role as previously, when it comes to oversight, enforcement and responding to complaints with regards to the data protection laws and those firms located solely in Ireland.

3.3 DATA PROTECTION OFFICER

Scouting Ireland has appointed a designated **DPO.** It has done so in accordance with the GDPR requirements and have ensured that the assigned person has an adequate and expert knowledge of data protection law. They have been assessed as being fully capable of assisting Scouting Ireland in

monitoring our internal compliance with the Regulation and supporting and advising employees and associated third parties with regards to the data protection laws and requirements. They can be contacted at dataprotection@scouts.ie or by ringing National Office on +353 (0)1 4956300.

4 OBJECTIVES

We are committed to ensuring that all personal data processed by Scouting Ireland is done so in accordance with the data protection laws and its principles, along with any associated regulations and/or codes of conduct laid down by the Supervisory Authority and local law. We ensure the safe, secure, ethical and transparent processing of all personal data and have stringent measures to enable data subjects to exercise their rights.

Scouting Ireland has developed the below objectives to meet our data protection obligations and to ensure continued compliance with the legal and regulatory requirements.

Scouting Ireland 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 Scouting Ireland, is monitored for compliance with the data protection laws and its principles
- Personal data is only processed where we have verified and met the lawfulness of processing requirements
- We only process special category data in accordance with the GDPR requirements
- We record consent, when necessary, at the time it is obtained and evidence such consent to the supervisory authority where requested
- All employees are competent and knowledgeable about their GDPR obligations and are provided with training in the data protection laws, principles, regulations and how they apply to their specific role and Scouting Ireland
- 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 maintain a continuous program of monitoring, review and improvement with regards to compliance with the data protection laws and to identify gaps and non-compliance before they become a risk, affecting mitigating actions where necessary
- We monitor the Supervisory Authority, European Data Protection Board (EDPB) and any GDPR news and updates, to stay abreast of changes, notifications and additional requirements
- We have robust and documented complaint handling and data breach process for identifying, investigating, reviewing, and reporting any breaches or complaints with regards to data protection
- We have appointed a **Data Protection Officer** who takes responsibility for the overall

supervision, implementation and ongoing compliance with the data protection laws and performs specific duties as set out under Article 37 of the GDPR

- We provide clear reporting lines and supervision with regards to data protection
- We store and destroy all personal information, in accordance with our retention schedule
- 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 in the form of a Privacy Notice
- Where applicable, we maintain records of processing activities in accordance with Article 30 requirements
- We have developed and documented appropriate technical and organisational measures and controls for personal data security

5 GOVERNANCE PROCEDURES

5.1 ACCOUNTABILITY & COMPLIANCE

We have implemented adequate and appropriate technical and organisational measures to ensure the safeguarding of personal data and compliance with the data protection laws and can evidence such measures through our documentation and practices.

Our main data protection 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 effective data protection training for all employees and volunteers as necessary.
- Identify key stakeholders to support the data protection compliance program
- Allocate responsibility for data protection compliance and ensure that the designated person(s) 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 Scouting Ireland 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 information policies and procedures.

5.1.1 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 have developed controls and measures *(detailed below*), that help us enforce this ethos.

Data Minimisation

Under Article 5 of the GDPR, principle (c) advises that data should be *'limited to what is necessary'*, which forms the basis of our minimalist approach. We only ever obtain, retain, process and share the data that is essential for carrying out our services and/or meeting our legal obligations and only retain data for as long as is necessary.

Our systems, processes and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to accomplish 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 includes: -

- 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 processors/controllers (*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
- Forms, contact pages and any documents used to collect personal information are reviewed annually or as necessary, to ensure they are fit for purpose and only obtain necessary personal information in relation to the legal basis being relied on and the purpose of processing

Anonymization

When sharing data to third parties, (such as the government or other monitoring agencies) where relevant or possible, we aim to anonymise the data, removing identifiers and separating permanently personal details or identifiers from the data sets. We aim to give only the basic, required data and no more, preserving the rights of the individual as much as possible. Special category data is restricted at all levels and can only be accessed by those who require using it to ensure the safety and welfare of the data subject and our members.

Encryption

We utilise encryption as a further risk prevention measure for securing the personal data that we hold. We utilise encryption 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 Officer is required to authorise the transfer and review the encryption method for compliance and accuracy.

Restriction

Our *Privacy by Design* approach means that we use company-wide restriction methods for all personal data activities. Restricting access is built into the foundation of Scouting Ireland'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 by those who require to use it to ensure the safety and welfare of the data subject and our members.

Hard Copy Data

Due to the nature of our business, it is sometimes essential for us to obtain, process, store and share personal and special category information which is only available in a paper format without pseudonymisation/anonymization options (*i.e. copies of Accident/Incident forms, Managing Medications Forms, Garda Vetting Forms, claims information*). Where this is necessary, we utilise a tiered approach to minimise the information we hold and/or the length of time we hold it for. ***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 feasible, 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 processer*) are verified and their identity and contact details checked
- The Data Protection Officer 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 appropriate *(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 Scouting Ireland, we use a physical, fire-proof, locked filing cabinet to store such documents as opposed to our standard archiving system

5.1.2 DATA PROTECTION AUDIT

To enable Scouting Ireland to fully prepare for and comply with the data protection laws, we have carried out a company-wide data protection audit to better enable us to record, categorise and protect the personal data that we hold and process.

The audit has identified, categorised and recorded all personal information obtained, processed and shared by our company 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

5.2 LEGAL BASIS FOR PROCESSING

At the core of all personal information processing activities undertaken by Scouting Ireland, is the assurance and verification that we are complying with Article 6 of the GDPR and our processing obligations. There are only 6 legal bases and these are described below. There are, however, any number of lawful purposes, so the GDPR does not try to list these – it limits itself to observing that any purpose for which data is processed must be lawful.

Prior to carrying out any personal data processing activity, we identify and establish the legal basis for doing so and verify these against the regulation requirements to ensure we are using the most appropriate legal basis.

The legal basis is documented on our information audit register and in our Privacy Notice and, where applicable, is provided to the data subject and supervisory authority as part of our information disclosure obligations. ***Data is only obtained, processed or stored when we have met the legal basis 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 Scouting Ireland
- Processing is necessary for the purposes of the "legitimate interests" pursued by Scouting Ireland 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).*

5.2.1 PROCESSING SPECIAL CATEGORY DATA

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

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.

Where Scouting Ireland processes any personal information classed as special category or information relating to criminal convictions, we do so in accordance with Article 9 of the GDPR.

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 defense 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)

Where Scouting Ireland processes personal information that falls into one of the above categories, we have adequate and appropriate provisions and measures in place prior to any processing. ***Measures include: -***

- Verifying our reliance on Article 9(1) GDPR prior to processing
- Documenting the Article 6(1) legal basis relied upon from processing on our Processing Activities Register (*where applicable)*

- 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

5.2.2 RECORDS OF PROCESSING ACTIVITIES

As an organisation with ***250 or more*** employees and members *(or where conditions 2,3,4 or 5 above apply*); Scouting Ireland maintains records of all processing activities and maintains such records in writing, in a clear and easy to read format and readily available to the supervisory authority upon request.

Acting in the capacity as a controller *(or a representative*), our internal records of the processing activities carried out under our responsibility, ***contain the following information: -***

- Our full name and contact details and the name and contact details of the Data Protection Officer. Where applicable, we also record any joint controller and/or the controller's representative
- The purposes of the processing
- A description of the categories of data subjects and of the categories of personal data
- The categories of recipients to whom the personal data has or will be disclosed *(including any recipients in third countries or international organisations)*
- Where applicable, transfers of personal data to a third country or an international organisation *(including the identification of that third country or international organisation and where applicable, the documentation of suitable safeguards)*
- Where possible, the envisaged time limits for erasure of the different categories of data
- A general description of the processing security measures as outlined in section 12 of this document *(pursuant to Article 32(1) of the data protection laws)*

5.3 THIRD-PARTY PROCESSORS

Scouting Ireland may from time to time 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 Scouting Ireland, 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
- Hosting or Email Servers

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

We engage with them 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 data subjects' rights and the security of their personal information is always priority when choosing a processor and we understand the importance of adequate and reliable outsourcing for processing activities as well as our continued obligations under the data protection laws for data processed and handled by a third-party.

5.4 DATA RETENTION & DISPOSAL

Scouting Ireland have defined procedures for adhering to the retention periods as set out by the relevant laws, contracts and our business requirements, as well as adhering to the GDPR 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 prioritises the protection of the personal data in all instances.

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

6 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 Scouting Ireland. We therefore utilise several measures and tools to reduce risks and breaches for general processing. However, where processing is likely to be high risk or cause significant impact to a data subject, we utilise proportionate methods to map out and assess the impact ahead of time.

Where Scouting Ireland 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)
- 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

7 Data Subject Rights

7.1 Consent & The Right to be Informed

The collection of personal and sometimes special category data is a fundamental part of the products/services offered by Scouting Ireland 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 law defines consent as; *'Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them.*

Where processing is based on consent, Scouting Ireland have reviewed and revised all consent mechanisms to ensure that: -

- Consent requests are transparent, use plain language and are 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, detailed 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 company 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 company 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
- Consent withdrawal requests are processed immediately and without detriment
- Where services are offered to children, age-verification and parental-consent measures have been developed and are in place to obtain consent
- 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

7.1.1 CONSENT CONTROLS

Scouting Ireland 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 and is documented in all instances.

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 those 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 Officer prior to being circulated.

Consent to obtain and process personal data is obtained by Scouting Ireland through: -

- Face-to-Face
- Telephone
- In Writing
- Email/SMS
- Electronic *(i.e. via website form*)

Any electronic methods of gaining consent are regularly reviewed and tested to ensure that a compliant Privacy Notice is accessible and displayed and that consent is clear, detailed and utilises a demonstrable opt-in mechanism. Where consent is obtained verbally, we utilise scripts, checklists to ensure that all requirements have been met and that consent is obtained compliantly and can be evidenced.

Electronic consent is always by a non-ticked, opt-in action where necessary (*or double opt-in where applicable*), enabling the individual to provide consent after the below information has been provided.

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.

7.1.2 ALTERNATIVES TO CONSENT

Scouting Ireland 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.

When reviewing the processing activity for compliance with the consent requirements, we ensure that none of the below are a factor: –

- Where we ask for consent but would still process it even if it was not given *(or withdrawn).* If we would still process the data under an alternative lawful basis regardless of consent, we recognise it is not the correct lawful basis to use
- Where we ask for consent to process personal data as a precondition of a service we are offering, it is not given as an option and consent is not appropriate

- Where there is an imbalance in the relationship, i.e. with employees

7.1.3 INFORMATION PROVISIONS

Where personal data is obtained directly from the individual *(i.e. through consent, by employees, 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 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 officer
- 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 Scouting Ireland intends to transfer the personal data to a third country or international organisation and the existence/absence of an adequacy decision by the Commission
    - where Scouting Ireland intends to transfer the personal data to a third country or international organisation without an adequate decision by the Commission, reference to the appropriate or suitable safeguards Scouting Ireland 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.

7.2 PRIVACY NOTICE

Scouting Ireland defines a Privacy Notice as a document, form, webpage or pop-up that 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 (*where collected directly from individual*) or *14 (where not collected directly)* requirements 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.

We have a link to our Privacy Notice on our website and provide a copy of physical and digital formats upon request. The notice is the member and public facing policy that provides the legal information on how we handle, process and disclose personal information.

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 as necessary
- Worded in full in agreements, contracts, forms and other materials where data is collected in writing or face-to-face as necessary
- In employee contracts and recruitment materials

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.

7.3 PERSONAL DATA NOT OBTAINED FROM THE DATA SUBJECT

Where Scouting Ireland obtains and/or processes personal data that has **not** been obtained directly from the data subject, such as in the case of emergency contact details or next of kin, Scouting Ireland must assume the personal details are provided with consent of the individuals involved. Due to the nature of Scouting Ireland, with underage members, we must assume that member give this necessary data with the consent of the data subject.

7.3.1 EMPLOYEE PERSONAL DATA

As per the data protection law guidelines, we do not use consent as a legal basis for obtaining or processing employee personal information. Our HR policies have been updated 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 and are provided with a Privacy Notice specific to the personal information we collect and process about them.

7.4 THE RIGHT OF ACCESS

We have ensured that appropriate measures have been taken to provide information referred to in Articles 13/14 and any communication under Articles 15 to 22 and 34 *(collectively, The Rights of Data Subjects*), 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*).

SARs are always completed within 30-days and are provided free of charge. However, where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended dependent on the complexity of the request and or the available resources. If this is the case, we will write to you within 30 days and keep you informed of the delay and provide the reasons.

Should the retrieval or provision of information be particularly unwieldly and or resource consuming we may request the subject to provide limits to the search. If this is the case, we will write to you within 30 days and keep you informed of any delay and provide the reasons.

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.

7.4.1 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 Scouting Ireland 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

7.5 RECTIFICATION & ERASURE

7.5.1 CORRECTING INACCURATE OR INCOMPLETE DATA

Pursuant to Article 5(d), all data held and processed by Scouting Ireland 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 Officer** is 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.

Where 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.

7.5.2 THE RIGHT TO ERASURE

Also, known as *'The Right to be forgotten'*, Scouting Ireland 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 Scouting Ireland 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.

7.6 THE RIGHT TO RESTRICT PROCESSING

There are certain circumstances where Scouting Ireland 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.

Scouting Ireland 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 of 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 Officer 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.

8 OVERSIGHT POLICY

8.1 SECURITY & 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. We 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 impact 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, Scouting Ireland 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).

9 TRANSFERS & DATA SHARING

Scouting Ireland 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 process that ensures such data is encrypted with a secret key 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 Officer authorises all EU transfers and verifies the encryption and security methods and measures.

10 AUDITS & MONITORING

This policy and procedure document details the extensive controls, measures and methods used by Scouting Ireland 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. In addition to these, we also carry out regular audits and compliance monitoring processes, with a view to ensuring that the measures and controls in place to protect data subjects and their information, are adequate, effective and compliant at all times.

The Data Protection Officer 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 Officer and copies provided to Senior Management and are made readily available to the supervisory authority where requested.

The aim of internal data protection audits is to: -

- Ensure that the appropriate policies and procedures are in place
- To verify that those policies and procedures are being followed
- To test the adequacy and effectiveness of the measures and controls in place
- To detect breaches or potential breaches of compliance
- To identify risks and assess the mitigating actions in place to minimise such risks
- To recommend solutions and actions plans to the board for improvements in protecting data subjects and safeguarding their personal data
- To monitor compliance with the data protection laws and demonstrate best practice

11 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. We are committed to ensuring new and existing employees are trained, assessed and supported and include: -

- GDPR Workshops & Training Sessions for employees and or relevant volunteers
- Access to GDPR policies, procedures, checklists and supporting and guidance documents
- Access to the DPO for support, assistance with questions and guidance

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

12 PENALTIES

Scouting Ireland understands its obligations and responsibilities under the data protection laws and recognises the severity of breaching any part of the law or Regulation. We respect the supervisory authority's authorisation under the legislation to impose and enforce fines and penalties on us where we fail to comply with the regulations, fail to 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. ***We recognise that: -***

- Breaches of the obligations of the controller, the processor, the certification body and the monitoring body, are subject to administrative fines up to €10,000,000 or 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- Breaches of the basic principles for processing, conditions for consent, the data subjects' rights, the transfers of personal data to a recipient in a third country or an international

organisation, specific processing situations (*Chapter IX*) or non-compliance with an order by the Supervisory Authority, are subject to administrative fines up to €20,000,000 or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

13 RESPONSIBILITIES

Scouting Ireland has appointed a **Data Protection Officer whose** role it is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees and upper management and to actively stay informed and up-to-date with all legislation and changes relating to data protection.

The DPO will work in conjunction with the Chief Executive Officer, IT Manager and Training Team to ensure that all processes, systems and staff are operating compliantly and within the requirements of the data protection laws and its principles.

The DPO 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 data protection training and will be subject to continuous development, support and mentoring to ensure that they are competent and knowledge for the role they undertake.

14 APPENDIX

14.1 DEFINITIONS

- ***"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 Scouting Ireland 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 they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them.
- ***"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 and any other relevant data protection laws that Scouting Ireland complies with.
- ***"Data subject"*** means an individual who is the subject of personal data
- ***"GDPR"*** means the *General Data Protection Regulation (EU) (2016/679)*
- ***"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 an independent public authority which is established by a Member State
- ***"Third Party"*** means a natural or legal person, public authority, agency or body other than the data subject, under our direct authority