General Data Protection Policy

V1.0 23 February 2018

Document Control

Approvals

This document requires approval from the following;

Approval Date	Title
	Executive Management Team
	Board of Management

Revision History

Revision Number	Revision Date	Changes from previous version	Author
1.0	N/A	New	Data and Records Manager

Location of Copies

Data and Records Management, SOI

Foreword

The mission of Special Olympics Ireland is to provide year-round sports training and athletic competition in a variety of Olympic-type sports for children and adults with an intellectual disability, giving them continuing opportunities to develop physical fitness, demonstrate courage, experience joy and participate in a sharing of gifts, skills and friendships with their families, other Special Olympics athletes and the community. Special Olympics Ireland is a registered charity (registered charity number CHY 7556).

Special Olympics Ireland's board and management are committed to preserving the confidentiality, integrity and availability of information. It pledges to respect people's rights to the protection of their personal information under the European Convention on Human Rights and the EU Charter of Fundamental Rights. It is within this context that Special Olympics Ireland, as a data controller, recognise our accountability under the General Data Protection Regulation 2016/679 (the "GDPR").

Everyone who works for, or with, Special Olympics Ireland is accountable for ensuring personal data is processed in compliance with all of the core principles and requirements of the GDPR. Special Olympics Ireland is compliant with the voluntary Governance Code for the community, voluntary and charity (CVC) sector. This includes identifying and complying with relevant legal and regulatory requirements. In terms of data protection this means that we must:

- Keep contact details of stakeholders with their permission in a safe place;
- Not give their details without their consent to someone outside the organisation;
- Not keep unnecessary personal information;
- Make sure our organisation complies with data protection legislation.

As part of our strategy for 2016-2020, Special Olympics Ireland is looking at how best to capture data and information and how to use and report on this data, in compliance with data protection legislation, but also in terms of efficiency and effectiveness. Good governance of information within our organisation maximises benefits for all of our stakeholders. Being aware of the risks to personal information and ensuring controls and mitigations are in place allows us to deliver on our personal information pledge.

Matt English

CEO - Special Olympics Ireland, Executive Office

February 2018

Contents

Approvals 2
Revision History 2
Location of Copies 2
1. Introduction 8
2. Objective 9
3. Scope 9
4. Policy 10
4.1. Responsibilities 10
4.2. Monitoring and review 10
4.3. Disciplinary Procedures 10
4.4. Overview of Data Protection 10
Confidentiality & non-disclosure 11
An individual's rights ..... **Error! Bookmark not defined.**
4.5. Governance and accountability 11
4.6. Privacy notices and statements 19
Email Disclaimer 19
4.7. Lawfulness of processing 19
Legal basis 19
Legitimate interest 19
Consent 19
Contract 20
4.8. Access and other requests 20
Subject Access Request log 21
Responding to the requester and timelines 21
Data and Records Manager 21
4.9. Privacy by Design and Default 21
Privacy by design 21
Privacy by default (need to know basis) 22
4.10. Data Processor and International Data Transfer Agreements 22
Data Processor Agreements 22
Transfers of personal data outside Europe 22
4.11. Data Security 23
4.12. Data Protection Impact Assessments 23
Methodology of the DPIA 23
DPIA Threshold Assessment 24

"Quality Gate" decisions 24
Full DPIA 24
Consultation with Data Subjects 24
Consultation with Data Processors 24
Prior consultation with the Data Protection Commissioner 25
Documentation of the DPIA process 25
4.13. Breach and Incident reporting 25
Breach log 25
Reporting an incident/ breach to the Data Protection Commissioner and timelines 25
Notification of the individual of an incident/ breach 26
Security breach response plan 26
Risk Register for potential breaches 26
4.14. Policies 26
Privacy Policies ..... **Error! Bookmark not defined.**
Direct Marketing Policy 27
Payment Processing Policy 27
Retention (and Destruction) of Data 27
Monitoring Policies 27
Acceptable Use – Internet and Email Policy 27
CCTV (Monitoring) Policy 28
4.15. Procedures which support data protection 28
Record of processing activities 28
Concerns raised by employees and volunteers 28
Complaints handling procedure 29
Data Champions 29
Data Protection Integrated Review Team 29
Audits 29
Clear desk and Tidy Friday 29
4.16. Training of Staff and Volunteers 29
4.17. Location of Policy 30
5. Associated Records 30
APPENDIX I ..... **Error! Bookmark not defined.**
APPENDIX II ..... **Error! Bookmark not defined.**
APPENDIX III ..... **Error! Bookmark not defined.**
APPENDIX IV ..... **Error! Bookmark not defined.**
APPENDIX V ..... **Error! Bookmark not defined.**
APPENDIX VI ..... **Error! Bookmark not defined.**

Definitions

GDPR Terminology	Definition
Processing	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.
Personal Data	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.
Data Concerning Health	Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.
Consent	'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.
Controller (data controller)	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.
Processor (data processor)	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain

GDPR Terminology	Definition
	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.
Restriction of Processing	The marking of stored personal data with the aim of limiting their processing in the future.
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Filing System	Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Binding Corporate Rules	Personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.
Third Party	A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Source: The GDPR (Article 4)

1. Introduction

Special Olympics Ireland (SOI) is committed to ensuring that personal data (also called "personal information") that we collect, process and use is managed with the highest standards of security and confidentiality, strictly in accordance with the Data Protection Acts 1988 and 2003 (Ireland), the Data Protection Act 1998 (UK) (the "Acts") and

General Data Protection Regulation 2016/679 (the “GDPR”). The registered office of SOI, the data “controller”, is based in the EEA. The policy applies to all personal information processed by the organisation relating to a living individual. Some of the key GDPR definitions, including “personal data”, are in the Definitions section at the beginning of this policy.

The data protection principles are revised under the GDPR but are broadly similar to the principles set out in Directive 95/46/EC (the “Data Protection Directive”) and the Acts. The GDPR builds upon the eight data protection principles under the Acts and the result is the seven core GDPR principles relating to processing of personal data. A new accountability principle, under the GDPR, makes SOI, as controller, responsible for demonstrating compliance with the data protection principles.

2. Objective

The purpose of this policy is to define SOI’s application of the GDPR principles relating to the manner in which it processes data organisation-wide. The policy applies to all personal data processed by the organisation, including athlete, website user and donor data as well as third party data, volunteer data and employee data.

The objective of this policy is to ensure that employees, volunteers, contractors and third party users are aware of the legal obligations governing personal data protection, their responsibilities and liabilities, and are equipped to support our Privacy Policies in

The seven core GDPR principles governing the processing of personal data are:

Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
Accuracy	Personal data shall be 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.
Storage limitation	Personal data shall be 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.
Integrity and confidentiality	Personal data shall be 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.

Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR.

3. Scope

The General Data Protection Policy is intended to serve as a general privacy policy which overviews how SOI applies the seven core GDPR principles organisation-wide. It is supported by a number of specific privacy policies which are relevant to the individual/ categories of personal data processed.

4. Policy

4.1. Responsibilities

SOI is responsible for making sure that our employees and volunteers understand their role, legal duties and delegated responsibility for decision-making in relation to personal information. Therefore, SOI employees and volunteers have responsibilities and liabilities to treat the personal information entrusted to SOI with the highest standard of confidentiality and to enable individuals to exercise their data protection rights in accordance with the Acts and the GDPR.

Employees and volunteers are accountable to the board through the CEO. In practice this means that both shall:

- Be aware of the location of the organisation's data protection policies, procedures, standards and guidelines;
- Act in line with the current data protection legislation;
- Comply with the relevant SOI policies.

4.2. Monitoring and review

SOI reserves the right to monitor and access all email, Internet and network use of users for legitimate business reasons including, but not limited to, compliance with organisational policy, compliance with any applicable laws and industry regulation or where there is reasonable suspicion of activities that may violate organisational policies. We engage in monitoring as per our Acceptable Use (Monitoring) Policy as well as CCTV (Monitoring) Policy.

4.3. Disciplinary Procedures

SOI has contracts and employment policies in place that cover disciplinary procedures. Failure to comply with the policies, procedures, standards and guidelines of SOI shall be reported and may result in disciplinary action.

4.4. Overview of Data Protection

We are all familiar with the concept of keeping information confidential and of being entrusted with secrets or private affairs. The terms "privacy", "data protection", and "information security" are often used. However, they may have different meanings depending on the context. Similarly, "privacy notice", "privacy statement" and "privacy policy" mean different things and are clarified below.

In Europe "data protection" is the term in the legal, policy and regulatory context which generally is referred to as "data privacy". These terms refer to the fundamental right of the individual to the protection of their personal information, especially in relation to the processing of their personal data.

Confidentiality & non-disclosure

Employees and volunteers shall maintain the confidentiality of information in order to protect company's data assets. They shall not disclose any unauthorised organisational information. They shall abide by requirements for confidentiality and non-disclosure even after leaving the employment or service of SOI.

4.5. Governance and accountability

Under the GDPR SOI, as controller, is obliged to demonstrate accountability for how we ensure our compliance. SOI has a number of governance processes in place as part of our compliance framework. In practical terms this includes the following:

- maintaining a record of processing activities under our responsibility;
- designing clear and informative privacy notices and statements;
- we have appointed a Data and Records Manager to which data protection related tasks are assigned;
- having written data processor agreements;
- ensuring that a Data Protection Impact Assessment has been run on any "high risk" processing activity (in particular IT projects involving new technologies) before it is commenced;
- regularly reviewing and monitoring the effectiveness of data protection policies and procedures.
- documenting how long we retain the categories of personal information belonging to the different categories of data subject;
- having a procedure for complaints handling;
- having periodic audits;
- preparing a personal information inventory as part of an ongoing data mapping project for SOI;
- ensuring that staff and volunteer receive personal data protection training and that it is tracked and documented;

4.6. General Data Protection Statement

Our Mission

The mission of Special Olympics Ireland (SOI) is to provide year-round sports training and athletic competition in a variety of Olympic-type sports for children and adults with an intellectual disability, giving them continuing opportunities to develop physical fitness, demonstrate courage, experience joy and participate in a sharing of gifts, skills and friendships with their families, other Special Olympics athletes and the community. SOI is a registered charity (registered charity number CHY 7556).

Record keeping

Under the GDPR SOI is required to keep a record of our personal information processing activities because we process "special categories" of information which athlete's health. This document is a statement of our commitment to data protection which includes details of the records we keep of our personal data processing activities under Article 30 of the GDPR.

Controller

The registered office of SOI, the data "controller", is based in the EEA.

Address:	Special Olympics Ireland Central Office, National Sports Campus, Snugborough Road, Dublin 15, D15 PC63, Ireland
Email:	info@specialolympics.ie
Telephone:	+353 1 882 3972 (reception)
Website:	www.specialolympics.ie

Data and Records Manager

SOI have appointed a Data and Records Manager to which data protection related tasks are assigned. Our Data and Records Manager is our point of contact with the Office of the Data Protection Commissioner and for anyone wishing to exercise their statutory data protection rights, such as making a subject access request to their personal data.

Name:	Elaine Hurley,
Address:	Special Olympics Ireland Central Office, National Sports Campus, Snugborough Road, Dublin 15, D15 PC63, Ireland
Email:	data@specialolympics.ie
Telephone:	+353 1 869 1614 (direct)

Registration of SOI with the Data Protection Commissioner

As per the Data Protection Commissioner guidelines, since 2007 not-for-profit charities are not obliged to register.

Purpose of processing

We collect individual's personal information for several purposes including:

Registering volunteer information on our website for re-vetting online and when volunteers register for specific SOI events and activities.

- Athlete registration: processing information collected on the Athlete Participation Form (APF) for the purpose of registration of the athlete with the programme care and for the welfare and safety of the athlete whilst at SOI events.
- Volunteer applications: processing volunteer applications completed online by website users as part of the volunteer process
- Volunteer medical information: applies to situations where SOI insurance contracts in order to determine who is responsible for payment pre-existing conditions as we know will fall under the remit of the volunteers own insurance or in instances when a medical incident occurs and the data subject is unable provide the information themselves
- Employee application records: processing any reference materials necessary to assess job applications
- Employee personnel and medical records: processing personal information as part of the employers contractual obligations
- Relationship management: maintaining our relationships with our donors, supporters, volunteers, athletes and their families using our and our customer relationship management (CRM) tool called Raiser's Edge
- Communication: registering of supporters for SOI events or activities online e.g. for a specific SOI update or for Connect Magazine (SOI "ezine")
- Marketing and fundraising management: processing of donor and supporter information on our CRM tool, for purposes including communicating our marketing and fundraising activities
- Management of donations and tax refunds: processing of donations by direct debit, by post, by cheque / bank draft / money order / bank lodgement. Sharing donor information (including by text or online) with our finance team for tax refunds
- Like many websites, the website uses session cookies that are transferred to your computer for the duration of your visit
- Analysis of website usage: some of the technical information captured on our website is used to create summary statistics to make our site more user-friendly
- Marketing and fundraising campaigns: some of our marketing emails have a tracking function used to help our marketers to gain insight into campaign performance
- CCTV footage for security, crime prevention and safety purposes

Categories of data subject

SOI processes personal information about individuals to help us fulfil our mission including:

- Former and current athletes and their families
- Donors and prospective donors
- Former and current employees
- Volunteers
- Supporters
- Anyone who makes a complaint or enquiry
- Visitors to SOI

Categories of personal data

The personal data which SOI processes relates to website user records, online volunteer application forms and hard copies of athlete forms, financial records and personnel records.

- The personal data which SOI processes includes: name, address, email, phone number, photographs and video footage.
- The "sensitive data" which we process concerns athlete, volunteer and employee medical information.
- The "high risk" information we process is financial information such as direct debit mandates.

Categories of recipients

SOI reserves the right to share the personal information of employees and volunteers on a collective basis with data processors to process data on our behalf.

SOI shall ensure that we have appropriate Data Processor Agreements (contracts) in place with our processors, ensuring processing be subject to suitable safeguards, in accordance with the requirements of the General Data Protection Regulation (GDPR).

SOI does not share personal information of employees and volunteers without their consent, unless allowed by legislation or for the performance of a contract.

Vetting disclosures are only used for the purpose for which they were provided to SOI in accordance with the consent of the vetting subject. The content of An Garda Síochána Vetting disclosures may involve sensitive personal information, however, they are not disclosed by An Garda Síochána Vetting to SOI.

The outcome of An Garda Síochána Vetting disclosures will not be further processed or disclosed by SOI to other parties even with consent.

Examples of organisations we may share personal information with, where appropriate, are:

Organisation	**Type of information shared**
An Garda Síochána	Garda Vetting Application Online; on applications made in Ireland
AccessNI	ID Validation; on applications made in Northern Ireland (NI)
Services	e.g. distribution of newsletters
LIKECHARITY	Service provider for SOI donate by text
Realex	Service provider for SOI online donations
Revenue Irish Tax and Customs	Tax relief on donations made in Ireland (ROI)
HM Revenue and Customs (HMRC)	Tax relief on donations made in NI

Transfers of personal data outside Europe

In certain cases it may be necessary for us to share personal information within the wider Special Olympics organisation including to regions outside of the European Economic Area (EEA). The privacy protections in these jurisdictions may not be equivalent to those in Europe. SOI will only transfer their personal data outside of the EEA where permitted to do so by European law and will take reasonable steps to ensure appropriate safeguards are put in place relating to the transfer. We do not share their information on a collective basis with regions outside the EAA unless we have the following arrangement(s) in place, including contracts where applicable, to process data on our behalf:

- Specific consent: to establish a new legal basis that will justify transatlantic data transfers e.g. opt-in sought;
- Approved certification schemes: US processors may self-certify to the standards set out in the Privacy Shield;
- Binding corporate rules: with Special Olympics and/ or Special Olympics Europe/Eurasia for intra-organisational transfers.

Transfers of personal data to recipients in "third countries" (i.e. outside of the European Economic Area ("EEA")) continue to be regulated and restricted in certain circumstances.

Examples of organisations outside the EAA that we share personal information with, where appropriate, are:

Organisation	**Type of information shared**	**Approved certification scheme(s): status***
MailChimp (The Rocket Science Group LLC d/b/a MailChimp)	Service provider for SOI marketing automation	EU-U.S. PRIVACY SHIELD FRAMEWORK: ACTIVE SWISS-U.S. PRIVACY SHIELD FRAMEWORK: ACTIVE
Blackbaud	Platform provider for CRM tool	EU-U.S. PRIVACY SHIELD FRAMEWORK: ACTIVE SWISS-U.S. PRIVACY SHIELD FRAMEWORK: ACTIVE
Microsoft Corporation	Platform provider for cloud computing	EU-U.S. PRIVACY SHIELD FRAMEWORK: ACTIVE SWISS-U.S. PRIVACY SHIELD FRAMEWORK: ACTIVE

* Source: https://www.privacyshield.gov/

Data Retention

SOI retains personal information in line with the purpose for which it was originally collected or lawfully further processed. We may retain personal information for a longer period of time if we are required to do by law in line with the Retention (and Destruction) Policy.

SOI's retention decisions are based on the following considerations:

- Historical value of the information: e.g. SOI's athletes have in many cases taken part in competitions representing Ireland and won medals.
- Legal or regulatory requirements: in some instances, for example financial records, the retention periods are fixed by the statutory retention period.
- Good practice: in other cases, there may not be statutory requirements, in which case SOI's decision is made on the basis of good practice.
- Administrative or operational needs: e.g. operational requirements may deem it necessary to retain SOI's athletes' Healthy Athlete Screening Forms, completed following health screening at events or Games, to retain this information for the entire 4 year event or games cycle (and an additional year for administrative purposes).

Examples of statutory retention periods for Ireland are summarised below:

Type of record (description)	**Retention Period**	**Why (Statutory or otherwise)**
Tax records	6 years (or more if the tax treatment of an item is in question. Records should be maintained until it is resolved)	Statutory
Accounting records	6 years (after the end of the financial year containing the latest date to which the record, information or return relates)	Statutory
Parental or force majeure leave records	8 years (from the period of leave) *NERA* (National Employment Rights Authority)	Statutory
Collective redundancies	3 years	Statutory
Employment records relating to persons under 18 years of age	3 years	Statutory
Employee's terms and conditions of employment	Duration of the employee's employment	Statutory

Type of record (description)	Retention Period	Why (Statutory or otherwise)
Employee payslips	3 years	Statutory
Timesheets	3 years	Statutory
Employee statement of their duties	3 years	Statutory
Accident report (adult)	10 years (from the period of accident)	Statutory
Accident Forms (minor)	Minimum of 20 years Until the minor turns 18 and then a further 10 years from the date of the accident or dangerous occurrence.	Statutory
Customer due diligence records	5 years (after the end of the relevant business relationship)	Statutory

Security of information

SOI industry standard technological processing safeguards to protect personal information. We have a number of physical security measures in place, such as office security and confidential destruction of all waste paper.

Personal information is data stored on secured servers hosted in Ireland with appropriate access permissions assigned to users. We also have interfaces with software providers who have self-certified under the EU-US Privacy Shield Framework. All SOI laptops and USB keys are encrypted. SOI is acutely aware of its responsibility to train employees and volunteers on their data protection responsibilities.

An individual's rights

Any personal information which an individual chooses to share with SOI will be treated with the highest standards of security and confidentiality, strictly in accordance with the current data protection legislation and the GDPR. These rights include:

- Right of access;
- Right to rectification;
- Right to be forgotten / erasure;
- Right to restrict processing;
- Right to object;
- Right to refuse automated decision making and/ or profiling;
- Right to portability.

An individual may contact our Data and Records Manager with regard to all issues related to the processing of their personal information and to exercise their rights under the GDPR. Individuals have the right to lodge a complaint with the Data Protection

Commissioner, the supervisory authority in Ireland where the operations of SOI, the data "controller", is based.

Contact Details for the Data Protection Commissioner

Postal Address (Portarlington Office): Canal House, Station Road, Portarlington, Co. Laois, R32 AP23, Ireland.
Email: info@dataprotection.ie
Telephone: +353 57 8684800 / +353(0)761 104 800 / Lo Call No. 1890 252 231
Fax: +353 57 868 4757
Website: https://www.dataprotection.ie

Thank you for reading our Data Protection Statement. If you have a query about this statement you may email us at data@specialolympics.ie or write to us through the Data and Records Manager contact details above.

4.7. Privacy notices and statements

A self-assessment privacy notice checklist is completed by our Data and Records Manager for every SOI privacy notice as part requirement of the General Data Protection Regulation (Articles 12, 13 and 14) and stored in the Data and Records Management Site File.

SOI has various privacy notices in place including the **Website Privacy Statement** and the website **Cookies Policy**. The SOI website cookie policy forms part of our overall privacy policy and covers the nature and use of cookies. SOI has separate privacy notices in place for the reference of our registered athletes, employees and volunteers such as the **Athlete Privacy Statement**, **Employee Privacy Statement** and the **Volunteer Privacy Statement**.

Email Disclaimer

SOI has a number of external privacy statements in place for the reference of the public, such as the **Email disclaimer**. Under the Companies Act (2014) we have an Email Disclaimer which includes reference to the email and attachments in the context of "privileged or confidential" information and how SOI "scans this material". The SOI email disclaimer is located at the bottom of each outgoing email.

4.8. Lawfulness of processing

These are the rules that SOI applies to our personal data processing activities;

- must have a legitimate basis (legal basis, legitimate interest, consent/ contract);
- comply with the principles of data protection and the GDPR ('lawfulness, fairness and transparency'; 'purpose limitation'; 'data minimisation'; 'accuracy'; 'storage limitation'; 'integrity and confidentiality' and 'accountability');
- relevant sectoral rules (special categories of data, e.g. health related information, transfers of data to third countries, e-privacy and marketing, the use of cookies);
- subjects have rights (information, access, rectification, objection);
- supervision & enforcement (Data Protection Commissioner & Courts).

Legal basis

SOI has a number of privacy policies in place which explain the purposes of the processing for which the personal data are intended. They include the legal basis for the processing which details how SOI, as data controller, uses the personal data of individuals within and external to the organisation.

In addition to our specific privacy policies, we have a number of sectoral policies that relate to the processing of personal information, e.g. our Direct Marketing Policy and our Payment Processing Policy.

Legitimate interest

SOI shall review the processing of personal data where legitimate interest is the basis of processing to determine if it is a targeted and proportionate way of achieving our purpose.

Consent

In order to ensure "fair" processing, SOI will ensure that the individual is provided with information in an open and transparent way. The basis of consent is an **informed** decision, specific and unambiguous. SOI will review any potential for a clear imbalance in power between our organisation and the individual when determining the extent that

consent is **freely** given. Silent consent, pre-ticked boxes or inactivity are examples of "implied consent" and are not an ethical data processing practice.

Table 1, below, includes a summary about the lawfulness of processing criteria.

Table 1: Lawfulness of Processing Criteria

Lawfulness of Processing Criteria	***Consent key criteria***
Personal data (non sensitive) (Art. 6)	*Consent is specific and captured at the appropriate time (e.g. at point of data capture).*
Special data categories (sensitive) (Art. 9)	*Explicit consent or a strict list of criteria under the GDPR including medical or health reasons or to protect the vital interests of the individual.* *Aim to also find alternative and/ or supplementary grounds for processing.*
Consent is the basis for processing (Art. 7)	*Consent must be freely given;* *May be removed as easily as it was given;* *Aim to also find alternative and/ or supplementary grounds for processing.*
Profiling (Art. 22)	*Consent must be an Opt-in choice;* *Adhere to the legislation on Privacy and Electronic Communications.*
Children's information (Art. 8)	*Validity of the manner in which the consent of the holders of parental responsibility over children is to be obtained;* *Language must be age appropriate.*

Contract

The final lawful basis where processing is necessary for the performance of a contract to which the data subject is a party; SOI processes employee personal and high risk information as part of the employers contractual obligations e.g. payment processing.

SOI recognises that formal contracts (Data Processor Agreements) must be in place with third party processors ensuring processing be subject to suitable safeguards and appropriate and organisational measures.

4.9. Access and other requests

The **Access (and Other Requests) Policy** explains how we at SOI support the individual in exercising their rights.

The rights of the individual are outlined in the individual's rights section of this policy. SOI employees and volunteers have associated responsibilities and liabilities to enable our customers exercise their rights under the data protection legislation. All requests must be made in writing. Individuals are not obliged to use our Subject Access Request Form, however, it will make the process more straightforward if we have some information about what it is they are looking for in particular. The right to have information provided to the individual in a portable format (portability) applies only to automated processing.

Subject Access Request log

Our Data and Records Manager will retain a log of all subject access requests. This log is stored electronically in a "confidential" folder. The log includes the name and contact details of the requester.

Responding to the requester and timelines

The individual's request shall be responded to within one month of the date the request was made. Our Data and Records Manager is responsible for dealing with all access requests, including those arising from An Garda Síochána, and relating to CCTV.

There are strict regulations around the legal basis for granting access. Any *"unauthorised disclosure of or access to personal data"* constitutes a data breach. Therefore, employees and volunteers shall not respond to access requests and must inform our Data and Records Manager in a timely manner.

Data and Records Manager

Our Data and Records Manager is our point of contact with the Office of the Data Protection Commissioner and for anyone wishing to exercise their statutory data protection rights, such as making a subject access request to their personal data.

Our Data and Records Manager reports directly to the Senior Director of Operations. SOI supports him/ her in performing their tasks within the organisation on a practical basis by providing:

- Access to other services e.g. Human Resources (HR) and Information Technology (IT)
- Communication of our Data and Records Manager role and activities to employees and volunteers
- Necessary resources are available to carry out role and activities
- Active support by senior management
- Adequate time to fulfil duties
- Access to personal data and processing operations
- Resources to maintain their expert data protection knowledge

External consultants, are available to SOI in the event of any incident that requires specialist advice.

4.10. Privacy by Design and Default

The concept of privacy by design is a fundamental basis of the Data Protection Impact Assessment (DPIA).

Privacy by design

The terms "privacy by design" and "data protection by design" mean the same thing, to take data protection into account in a well-defined manner throughout any process. SOI is obliged under the GDPR to adopt significant new technical and organisational measures to demonstrate compliance. The focus under the GDPR is therefore on the

individual rather than the organisation. Below is our approach to implementing people, process and technological safeguards to implement data protection principles.

Privacy by default (need to know basis)

Employees and volunteers are encouraged by SOI to review the personal data they access to determine if the data is being processed on a need to know basis. SOI has a process for reporting concerns around the data that either they themselves or colleagues have access to.

As part of SOI's approach to "privacy by default" for manual files, we require employees and volunteers to ensure that their workspace is cleaned of paper information that is of a privileged or confidential nature, and kept locked away, while away from their desk in accordance with our Clear Desk and Tidy Friday procedures.

4.11. Data Processor and International Data Transfer Agreements

SOI is aware of our responsibility, as data controller, to have formal contracts (Data Processor Agreements) in place with third party processors ensuring processing be subject to suitable safeguards and appropriate and organisational measures.

Data Processor Agreements

SOI requires an agreement by the processor to adhere to data protection principles and specific requirements under the GDPR including:

- to process the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation;
- to have committed to confidentiality;
- to not engage another processor (sub-processor) without prior specific or general written authorisation of the controller;
- to ensure sub-processors process the personal data only on documented instructions from the controller;
- to put in place technical and organisational measures;
- at the choice of the controller, deletes or returns all the personal data to the controller;
- to allow for and contribute to audits and
- to immediately inform the controller if, in its opinion, an instruction around making information available to demonstrate compliance infringes data protection provisions.

SOI may assign the creation of data processor agreements and amendments to an external consultant. Data Processor agreements must be in writing and be approved by SOI's Data and Records Manager.

Transfers of personal data outside Europe

In certain cases it may be necessary for us to share their data within the wider Special Olympics organisation including to regions outside of the European Economic Area (EEA). The privacy protections in these jurisdictions may not be equivalent to those in Europe. We will only transfer their personal data outside of the EEA where permitted to do so by European law and will take reasonable steps to ensure appropriate safeguards are put in place relating to the transfer. We do not share their information on a collective basis with regions outside the EAA unless we have the following arrangement(s) in place, including contracts where applicable, to process data on our behalf:

- Specific consent: to establish a new legal basis that will justify transatlantic data transfers e.g. opt-in sought;
- Approved certification schemes: US processors may self-certify to the standards set out in the Privacy Shield;
- Binding corporate rules: with Special Olympics and/ or Special Olympics Europe/Eurasia for intra-organisational transfers.

Transfers of personal data to recipients in "third countries" (i.e. outside of the European Economic Area ("EEA")) continue to be regulated and restricted in certain circumstances.

4.12. Data Security

Both "data security" and "information security" refer to a number of industry standard technical and organisational security measures that SOI, as controller, within the meaning of that term in the Acts and the GDPR, has in place to protect personal data. In Ireland, some of the requirements relating to "security of processing" are governed by the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (the 2011 Regulations). In the UK this is covered by the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("the PECR").

SOI employees and volunteers have associated responsibilities and liabilities to keep the personal information entrusted to SOI secure and to report all information security weaknesses or incidents. Further information relating to the security measures may be found in the **Information Security Policy**.

4.13. Data Protection Impact Assessments

The terms "privacy impact assessment" (PIA) and "data protection impact assessment" (DPIA) are used interchangeably. However, they have the same meaning. Whether it is implementing a new system (in particular IT projects involving new technologies), or a change in business process, the DPIA is a governance tool that supports organisational planning and it used to identify any impact on the handling of personal data irrespective of to whom it relates. The DPIA, under the GDPR, is a "risk based" approach to compliance.

A DPIA is an assessment SOI shall use to identify and minimise non-compliance risks. A DPIA is, in particular, required for processing activities such as monitoring of a publicly accessible area on a large scale, systematic and extensive evaluations (e.g. profiling) or large scale of special categories, often referred to as sensitive data; (e.g. data concerning health).

A DPIA Threshold Assessment is completed by the SOI key contact for the project, system or process that DPIA document relates as part requirement of the General Data Protection Regulation (Article 35) and stored in the Data and Records Management Site File.

It is the task of the SOI key contact for the project, system or process that DPIA document relates, not our Data and Records Manager, to complete the details required in the DPIA document. SOI employees must seek the advice of our Data and Records Manager when carrying out a DPIA.

Methodology of the DPIA

DPIAs are mandatory under the GDPR and in SOI they are part of our documented approach to compliance and a point where we review our Risk Register for Potential Breaches. The DPIA process in SOI has two components or a two stage test, namely,

the DPIA Threshold Assessment and the full DPIA. DPIAs must be informed by privacy by design.

We use DPIAs at SOI for the following reasons:

- Good practice;
- Legal requirement;
- Risk management;
- Cost saving and;
- Supports organisational learning;
- Record Keeping.

DPIA Threshold Assessment

A DPIA threshold assessment is completed by our Data and Records Manager for every SOI privacy notice as part requirement of the General Data Protection Regulation (Articles 12, 13 and 14) and stored in the Data and Records Management Site File.

This DPIA threshold assessment is an initial assessment of risk-impact on privacy with YES, NO or UNCERTAIN response options. The requirement to perform a DPIA is conditional on the response to each of the questions.

"Quality Gate" decisions

There is role for a "critical" element in the decision-making process. It is important that "Group Think" is avoided. It is vital that any of our stated "legitimate business interest" arguments are challenged in situations where they are the sole basis of our processing activity.

Full DPIA

In practice, the full DPIA document is a business plan which includes the following components;

Goals: A description of the processing activities and their purpose and, where applicable, the legitimate interest pursued by the controller.

Assessment: An assessment of the need for and proportionality of the processing operations.

Risk (privacy and other rights): An assessment of the risks arising and measures adopted to mitigate those risks, including;

- Risk to organisation
- Risk to individual, fundamental human rights basis – impact on other rights e.g. choices people make.

Consultation with Data Subjects

SOI is keen that our employees and volunteers engage in the role of "devil's advocate" and speak up for the privacy rights of themselves and the individuals (including children and vulnerable persons). The Data Protection Integrated Review Team has a role in the DPIA process in representing the "voice of customer" (VOC) where appropriate.

Consultation with Data Processors

The data processor, where applicable, should be requested to assist SOI in ensuring compliance with the obligations deriving from the carrying out of DPIAs and from prior consultation of the Data Protection Commissioner.

Prior consultation with the Data Protection Commissioner
There are strict regulations around risk response including the criteria for informing the individual and the Data Protection Commissioner.

If the DPIA indicates a "high" risk to the individual AND there are no measures to mitigate (or reduce) the risk, then our Data and Records Manager will be obliged to consult with the ODPC. Therefore, employees and volunteers must include our Data and Records Manager at an early stage AND throughout the DPIA process.

Documentation of the DPIA process
The entire DPIA process should be documented with senior management approval, and stored in our Data and Records Management Site File.

4.14. Breach and Incident reporting
Employees and volunteers shall report all data breaches or incidents to SOI's IT Department in line with the **Security Breach Response Plan**.

Examples of events related specifically to personal data breaches include, but are not limited to, unauthorised access attempts to or use of a system or data, changes to the configuration of hardware or software without the consent of the IT Department and potential non-compliance with organisation policies and procedures.

A data security breach can happen for a number of reasons including:

- loss or theft of data or equipment on which data is stored;
- inappropriate access controls allowing unauthorised use;
- equipment failure;
- human error;
- unforeseen circumstances such as a fire or flood;
- hacking attack;
- 'blagging' offences where information is obtained by deceiving the organisation who holds it.

Further examples may be found in the Security Breach Response Plan.

Breach log
SOI's IT Department shall inform our Data and Records Manager of all breaches reported to them to enable him/ her to keep a log of data breaches. All data breaches shall be logged by our Data and Records Manager regardless of whether or not they are reported to the Data Protection Commissioner and/ or the individual.

Reporting an incident/ breach to the Data Protection Commissioner and timelines
Certain data breaches must be reported to the Data Protection Commissioner within 72 hours of the event. A detailed procedure may be found in the **Security Breach Response Plan**. Our Data and Records Manager is responsible for dealing with all suspected data breaches, regardless of whether or not they are reported to the Data Protection Commissioner and/ or the individual.

There are strict regulations around risk response including the criteria for informing the individual and the Data Protection Commissioner. It is imperative that the consequences of the risk and measures taken or to be taken to deal with the breach. Therefore, employees and volunteers shall not respond to access requests and must inform both our Data and Records Manager and IT of any suspected breach as soon as possible.

Notification of the individual of an incident/ breach

There are certain conditions where the individual must be informed under the GDPR and this must be without undue delay.

Security breach response plan

SOI's process for dealing with a breach (disaster) recovery plan will incorporate the following components:

- Reporting to the Data Protection Commissioner
- Timelines
- Investigation, likely consequences and mitigation strategy
- Involvement of the data processor, where applicable
- Notification to individuals

This is a risk-based document and will include having a risk register.

Risk Register for potential breaches

As part of the Security Breach Response Plan, our Data and Records Manager will, in consultation with the IT Department, create and maintain a Data Management Risk Register for potential data breaches. This risk register is also reviewed as part of our DPIA process.

The SOI risk register for any potential data breaches considers the following components:

- identify the risk categories;
- the specific risks related to each category;
- whether each category might become a reality;
- the consequences of the risk occurring;
- who in the company has responsibility for handling the risk;
- the likelihood of the risk occurring;
- likely severity;
- efforts undertaken to ameliorate the risk;
- risk that remains after mitigation efforts have been undertaken and;
- further necessary actions.

4.15. Policies

This section summarises SOI's policies which relate to the processing of personal information. All of our policies are reviewed by the SOI EMT (Executive Management Team) prior to approval by our Board.

The following policies are published on the SOI website: (www.specialolympics.ie)

- Terms and Conditions
- General Data Protection Policy
- CCTV (Monitoring) Policy
- Website Privacy (located at the "Privacy Policy" link)
- Cookies

The below key policies are available on the SOI shared drive.

- Privacy Statements (Employee, Volunteer, Athlete)
- Direct Marketing
- Payment Processing
- Retention (and Destruction) of Data
- Information Security

- Access (and Other Requests) Policy
- Acceptable Use (Monitoring)

Direct Marketing Policy

The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest of SOI as a not-for-profit charity. The legal basis for processing is an individual's free and informed consent. Consent to processing will include action taken by the individual to "Opt-in". In accordance with policy, an individual will be provided with regular opportunities to "unsubscribe" to direct marketing.

Where personal data are processed for direct marketing purposes, an individual will have the right to object at any time to processing of their personal data for such marketing. SOI plans to have a **Direct Marketing Policy** in place by the end of Q2 of 2018.

Payment Processing Policy

SOI processes high risk personal information such as financial data. SOI's policy is that this, and all personal information, shall be processed only for the specific purpose(s) for which it was obtained. The basis of processing this the performance of a contract to which the data subject is a party.

We do not share financial information on a collective basis with third party data processors unless we have a written Data Processor Agreement in place with them to process data on our behalf in line with our **Payment Processing Policy**.

Retention (and Destruction) of Data

We retain personal information in line with the purpose for which it was originally collected or lawfully further processed. We may retain personal information for a longer period of time if we are required to do by law. Departments/ individuals shall ensure that information is held for no longer than is necessary for the purposes for which the personal data was collected in line with the **Retention (and Destruction) Policy**.

Monitoring Policies

The Acceptable Use – Internet and Email and the CCTV policies relate to the monitoring of the public, and in particular employees and volunteers, for security, crime prevention and safety purposes.

Acceptable Use – Internet and Email Policy

Employees and volunteers shall not have an expectation of absolute privacy with regard to any activities performed or materials that are created, sent or stored using or on the organisation's information systems.

Employees and volunteers shall comply with the Information Security Policy when utilising SOI's information systems for processing personal information for business purposes. SOI's revised **Acceptable Use Policy** includes the use of personal devices in its scope.

BOYD Policy- Accessing and Storing SOI data on personal devices

The BYOD (Bring Your Own Device Policy) refers to the accessing and storing of SOI data on personal devices. Personal devices include mobile phones, iPads, laptops, tablets, PCs or other personal mobile devices.

No personal devices are allowed onto the SOI corporate network. Personal devices may be used to access SOI data only via web-based applications, e.g. Sharepoint and Email hosted on Microsoft Office 365. Only staff and volunteers with appropriate user rights may access SOI Data. Sensitive SOI Data should never be shared with unauthorised users.

Employees and volunteers who **opt-in** to the BYOD Policy must delete SOI data from their personal devices once the purposes for which SOI has disclosed it to them has finished. They are required to provide SOI with permission to delete it, if necessary.

Employees and volunteers who **opt-in** to use their own devices to access or store SOI data on their own devices shall put in place measures to safeguard the information, i.e. have a start-up password/pin on their device and set it to lock if not active for a specified period of time.

If employees and volunteers opt-out from the Bring Your Own Device Policy, they are not permitted to access or store SOI data on their personal devices.

CCTV (Monitoring) Policy

The CCTV Policy details how SOI, as data controller, uses the personal data of individuals within and external to the organisation. SOI reserves the right to utilise CCTV to monitor the perimeter of the SOI Office on the National Sports Campus and other property on its premises for security purposes. The National Sports Campus manages the processing of CCTV footage (images with the capacity to recognise faces) on our behalf.

SOI reserves the right, under certain circumstances, to authorise the disclosure CCTV footage with An Garda Síochána (employees and volunteers shall, at all times, only accede to a formal written request stating the legal basis for the disclosure).

Employees and volunteers shall refer to the CCTV Policy for details of the retention period for CCTV and how an individual may exercise their statutory data protection rights in relation the processing of CCTV footage. SOI plans to have a **CCTV Policy** in place by the end of Q2 of 2018.

4.16. Procedures which support data protection

SOI appreciates the importance of documenting our decision-making and due process; *"If It's Not Written, It Wasn't Done".* In the context of the GDPR this is particularly important because there is a sub-category of personal data known as "special categories" (or sensitive data) of information which relates to processing personal data concerning health. The "sensitive data" which SOI processes concerns athlete's medical information.

Record of processing activities

Under the GDPR, the records that are required by SOI to demonstrate compliance are detailed in our General Data Protection Statement.

Concerns raised by employees and volunteers

As part of the Governance Code, SOI has arrangements in place for employees and volunteers to raise concerns in confidence about possible improprieties relating to data protection. This policy is in line with the Protected Disclosures Act (2014).

Employees and volunteers may report concerns directly to our Data and Records Manager. Our Data and Records Manager is bound by "*discretion and confidentiality*" concerning his/ her tasks. He/ she is obliged under the GDPR, to keep a log of Subject

Access Requests and a log of Breaches. They are saved electronically in a **confidential** folder on the SOI shared drive that has restricted access rights. In addition to our Data and Records Manager, is also accessible to the Senior Director of Operations, IT Manager and the SOI IT Support Team. Under certain circumstances, our Data and Records Manager/ SOI are required to inform the Data Protection Commissioner and the individual of data incidents and breaches.

Complaints handling procedure
An individual may contact our Data and Records Manager to seek a resolution of the complaint or enquiry in the first instance. Further information about how SOI manages complaints is contained in our **Complaints Policy**.

An individual has the right to lodge a complaint with the Data Protection Commissioner who is responsible for upholding the privacy rights of individuals in relation to the processing of their personal data.

Data Champions
SOI understands the importance sharing the data protection message throughout the organisation. Our Data Champions are made up of employees and volunteers from departments in central office and a representative from the regional offices. Data Champions support and advise colleagues on the proper handling of personal information data. They help our Data and Records Manager to promote good data management practice and the GDPR principles for data processing.

Data Protection Integrated Review Team
The data protection integrated review team (data protection IRT) is set up on a project by project basis with the purpose of assisting SOI management in the carrying out of Data Protection Impact Assessments, where necessary.

Audits and data mapping
SOI reserves the right to perform audits, or engage with third party consultants to do so, each year (unannounced) and report the findings to the Board.

The method used to populate SOI's Data Map is "Questionnaires & Interview". The Data and Records Manager is responsible for creating a Data Inventory Questionnaire for completion by each SOI department. It is the responsibility of each of SOI departments to fully support the Data and Records Manager in assigning roles and responsibilities for the ongoing project of data mapping.

Clear desk and Tidy Friday
In order to reduce the risks of unauthorised access, loss of, and damage to information during and outside normal working hours, SOI requires that information is cleared away at the end of the working day and screens are clear.

Departments/ individuals will set aside approximately 30 minutes of the last Friday of every month ("*Tidy Friday*") for a company-wide office clearing session that includes clearing workspaces and departmental storage facilities. Departments/ individuals shall destroy privileged or confidential information in line with the Retention (and Destruction) Policy.

4.17. Training of Staff and Volunteers
Data Protection Training will be provided to employees and volunteers and will be supported by online resources and information sheets. Refresher training will be provided every two years and as directed by their line manager. Under the GDPR, the agenda for SOI training may, as appropriate, include the following;

- The GDPR Principles for processing personal information
- Categorise of data (e.g. children's, special categories, high risk)
- Role of our Data and Records Manager
- Legal basis for processing (consent, legitimate business interest etc.)
- Data Protection Impact Assessments (questionnaires, review, content of DPIAs)
- Privacy by design
- Breaches, timelines and logging
- Access requests, new timelines, new fee changes, format of requests and logging
- Contracts with processors
- Employee and customer privacy – monitoring, location of policies

SOI may assign the creation of, and providing the training to an external consultant. SOI is responsible for ensuring that training is tracked and that the content of the training is documented for our records.

Employees and volunteers shall revert to the SOI's HR Manager and our Training Manager to ensure that this training is tracked and that the content of the training is documented for our records.

4.18. Location of Policy

A copy of this policy is kept on file by our Data and Records Manager. It is also published on the SOI website: (www.specialolympics.ie)

5. Associated Records

The following records are associated with this policy.

- Website Terms and Conditions
- General Data Protection Policy
- CCTV Policy
- Website Privacy
- Cookies Policy
- Privacy Statements (Employee Privacy, Volunteer, Athlete)
- Direct Marketing Policy
- Payment Processing Policy
- Retention (and Destruction) of Data Policy
- Information Security Policy
- Access (and Other Requests) Policy
- Acceptable Use Policy

Declaration of General Data Protection Policy

I have read and understood the Special Olympics Ireland General Data Protection Policy. Updates to the current version will be notified to all users if/when they occur. The most up to date version of the policy will be published on the shared drive within the Policies and Procedures folder. If I am in any doubt about whether any aspect of my processing of personal information complies with the General Data Protection Policy, I will refer to the current version and/ or discuss the matter with my manager.

Failure to comply with the policies, procedures, standards and guidelines of SOI shall be reported and may result in disciplinary procedures.

Disciplinary procedures may include, but is not limited to, reprimand, financial penalties, dismissal from voluntary service, termination of employment, and/or legal action.

Signature: _____ Date: _____

Print Name: _____