Data Protection Policy

Our Policy

Special Olympics Great Britain ("**Special Olympics GB**") is committed to complying with data protection law and to respecting the privacy rights of individuals. The policy applies to all of our athletes, staff, workers, directors, volunteers and consultants ("**Members**").

The Data Protection Act 1998 ("**DPA**") applies to any personal data that we process, and from 25th May 2018, will be replaced by the General Data Protection Regulation ("**GDPR**") and the Data Protection Act 2018 ("**DPA 2018**") (together "data protection laws") and then after Brexit the UK will adopt laws equivalent to these data protection laws.

This Policy is written as though GDPR and the DPA 2018 are both in force, i.e. it states the position as from 25th May 2018.

The data protection laws require that personal data is processed in accordance with the Data Protection Principles and gives individuals rights to access, correct and control how we use their personal data.

This Data Protection Policy ("**Policy**") sets out our approach to data protection law and the principles that we will apply to our processing of personal data. The aim of this Policy is to ensure that we process personal data in accordance with the law and with the utmost care and respect. The Policy applies to

- the national office of Special Olympics GB; athletes, volunteers, and paid staff
- its accredited programmes;
- all Special Olympics GB donors, sponsors, and supporters; and
- any other person, persons, entity or entities doing work for or on behalf of Special Olympics GB.

References in this Policy to "*us*", "*we*", "*ourselves*" and "*our*" are to Special Olympics GB and all its Accredited Programmes. References to *"you", "yourself"* and *"your"* are to each Member to whom this Policy applies.

We recognise that you have an important role to play in achieving these aims. It is your responsibility, therefore, to familiarise yourself with this Policy and to apply and implement its requirements when processing any personal data.

Data protection law is a complex area. This Policy has been designed to ensure that you are aware of the legal requirements imposed on you and on us and to give you practical guidance on how to comply with them. This Policy also sets out the consequences of failing to comply with these legal requirements. However, this Policy is not an exhaustive statement of data protection law nor of our or your responsibilities in relation to data protection.

If at any time you have any queries on this Policy, your responsibilities or any aspect of data protection law, seek advice. Contact your line manager or the Data Protection Officer, Peju Oriunuta.

1. **Definitions**

The Data Subject is the living individual whose personal data is being processed.

Examples include:

- athletes;
- employees – current and past;
- volunteers;
- job applicants;
- sponsors/donors;
- users; and

- suppliers.

Processing means the use made of personal data including:

- obtaining and retrieving;
- holding and storing;
- making available in furtherance of Special Olympics GB's objectives; and
- printing, sorting, matching, comparing, and destroying.

The Data Controller - the legal 'person', or organisation, that decides why and how personal data is to be processed. The Data Controller is responsible for complying with the Data Protection Law.

The Data Processor - the Data Controller may get another organisation to be their data processor, in other words to process the data on their behalf. The responsibility of what is processed and how, remains with the Data Controller and the data processor must faithfully comply with the Data Controller's instructions. Special Olympics GB aims to always put in place a written contract with the Data Processor who must have appropriate security.

The Data Protection Officer - the name given to the person in organisations who is the central point of contact for all data compliance issues.

2. **Who is responsible for data protection?**

The Board of Trustees recognises its overall responsibility for ensuring that Special Olympics GB complies with its legal obligations.

Each member of staff, and volunteer at Special Olympics GB who handles personal data will comply with the organisation's operational procedures for handling personal data (including induction and training) to ensure that good data protection practice is established and followed.

Each accredited programme committee is responsible for their programme's compliance with this policy and supporting guidance.

All staff and volunteers are required to read, understand, and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

The Data Protection Officer is currently Peju Oriunuta, who has the following responsibilities:

- Briefing the board on Data Protection responsibilities
- Reviewing data protection and related policies
- Advising staff and SOGB membership on Data Protection issues
- Ensuring that data protection induction and training takes place
- Handling subject access requests
- Approving non-standard disclosures of personal data
- Ensuring contracts with Data Processors have appropriate data protection clauses
- Ensuring data protection statement is uploaded and displayed on the website and online shop
- Approving data protection-related statements on publicity materials and letters

3. **Status of this Policy and the implications of breach.** We recognise that processing of individuals' personal data in a careful and respectful manner cultivates trusting

relationships with those individuals and trust in our brand. We believe that such relationships will enable our organisation to work more effectively with and to provide a better service to those individuals.

This Policy works in conjunction with other policies implemented by us from time to time. All Members must read this Policy carefully and make sure they are familiar with it. Any breach of this Policy is a disciplinary offence and will be dealt with under Special Olympics GB's disciplinary procedures.

If you do not comply with data protection laws and/or this Policy, then you are encouraged to report this fact immediately to our Data Protection Officer. This self-reporting will be taken into account in assessing how to deal with any breach, including any non-compliance which may pre-date this Policy coming into force.

Also if you are aware of or believe that any other representative of ours is not complying with data protection laws and/or this Policy you should report it in confidence to our Data Protection Officer.

4. **Other consequences**

There are a number of serious consequences for both yourself and us if we do not comply with data protection laws. These include:

For you:

Disciplinary action: If you are an employee, your terms and conditions of employment require you to comply with our policies. Failure to do so could lead to disciplinary action including dismissal. Where you are a volunteer, failure to comply with our policies could lead to termination of your volunteering position with us.

Criminal sanctions: Serious breaches could potentially result in criminal liability.

Investigations and interviews: Your actions could be investigated and you could be interviewed in relation to any non-compliance.

For the organisation:

Criminal sanctions: Non-compliance could involve a criminal offence.

Civil Fines: These can be up to Euro 20 million or 4% of group worldwide turnover whichever is higher. These amounts are very substantial.

Assessments, investigations and enforcement action: We could be assessed or investigated by, and obliged to provide information to, the Information Commissioner on its processes and procedures and/or subject to the Information Commissioner's powers of entry, inspection and seizure causing disruption and embarrassment.

Court orders: These may require us to implement measures or take steps in relation to, or cease or refrain from, processing personal data.

Claims for compensation: Individuals may make claims for damage they have suffered as a result of our non-compliance.

Bad publicity: Assessments, investigations and enforcement action by, and complaints to, the Information Commissioner quickly become public knowledge and might damage our brand. Court proceedings are public knowledge.

Use of management time and resources: Dealing with assessments, investigations, enforcement action, complaints, claims, etc. takes time and effort and can involve considerable cost.

5. **Data protection laws**

The main themes of the data protection laws are:

- good practices for handling personal data;
- rights for individuals in respect of personal data that data controllers hold on them; and
- being able to demonstrate compliance with data protection laws.

In summary, the data protection laws require us to:

- only process personal data for certain purposes;
- process personal data in accordance with the 6 principles of 'good information handling' (including keeping personal data secure, processing it fairly and in a transparent manner and keeping it for no longer than is required);
- provide certain information to those individuals about whom we process personal data which is usually provided in a privacy notice, which will be on Special Olympics GB data-gathering forms;
- respect the rights of those individuals about whom we process personal data (including providing them with access to the personal data we hold on them); and
- keep adequate records of how data is processed and, where necessary, notify the regulator and possibly data subjects where there has been a data breach.

Every Member has an important role to play in achieving these aims. It is your responsibility, therefore, to familiarise yourself with this Policy.

Data protection law in the UK is enforced by the Information Commissioner's Office ("**ICO**") and they are the regulator for data protection in the UK. The ICO has extensive powers, including the ability to impose civil fines of up to Euros 20 million or 4% of group worldwide turnover, whichever is higher. Also the data protection laws can be enforced in the courts and the courts have the power to award compensation to individuals.

6. **Data protection principles**

The data protection laws set out 6 principles for maintaining and protecting personal data, which form the basis of the legislation. All personal data must be:

- processed lawfully, fairly and in a transparent manner and only if certain specified conditions are met;
- collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes ("**purpose limitation**");
- adequate and relevant, and limited to what is necessary to the purposes for which it is processed ("**data minimisation**");
- accurate and where necessary kept up to date;
- kept for no longer than is necessary for the purpose ("**storage limitation**");
- processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures ("integrity and security").

7. **Data subject rights**

Under data protection laws individuals have certain rights in relation to their own personal data. In summary these are:

- The rights to access their personal data, usually referred to as a subject access request;
- The right to have their personal data rectified;
- The right to have their personal data erased, usually referred to as the right to be forgotten;
- The right to restrict processing of their personal data;
- The right to object to receiving direct marketing materials;
- The right to portability of their personal data;
- The right to object to processing of their personal data; and
- The right to not be subject to a decision made solely by automated data processing.

8. **Your main obligations**

- What this all means for you can be summarised as follows:
- Treat all personal data with respect;
- Treat all personal data how you would want your own personal data to be treated;
- Immediately notify your line manager or our Data Protection Officer if any individual says or does anything which gives the appearance of them wanting to invoke any rights in relation to personal data relating to them;
- Take care with all personal data and items containing personal data you handle or come across so that it stays secure and is only available to or accessed by authorised individuals; and
- Immediately notify our Data Protection Officer if you become aware of or suspect the loss of any personal data or any item containing personal data. [For more details on this see our separate Data Security Breach Policy which applies to all Members regardless of their position or role in our organisation].

9. **Your activities**

Data protection laws have different implications in different areas of our organisation and for different types of activity, and sometimes these effects can be unexpected.

Areas and activities particularly affected by data protection laws include Human Resources, payroll, security (e.g. CCTV), member/customer support, sales, data inputting, promotions, health and safety, finance, performance and participation

You must consider what personal data you might handle, consider carefully what data protection laws might mean for you and your activities, and ensure that you comply at all times with this policy.

10. **Practical matters**

Whilst you should always apply a common sense approach to how you use and safeguard personal data, and treat personal data with care and respect, set out below are some examples of dos and don'ts:

- Do not take personal data out of the organisation's premises (unless absolutely necessary).
- Only disclose your unique logins and passwords for any of our IT systems to authorised personnel (e.g. IT) and not to anyone else.

- Never leave any items containing personal data unattended in a public place, e.g. on a train, in a café, etc. and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.
- Never leave any items containing personal data in unsecure locations, e.g. in car on your drive overnight and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.
- If you are staying at a hotel then utilise the room or hotel safe to store items containing personal data when you do not need to have them with you.
- Do encrypt laptops, mobile devices and removable storage devices containing personal data.
- Do lock laptops, files, mobile devices and removable storage devices containing personal data away and out of sight when not in use.
- Do password protect documents and databases containing personal data.
- Never use removable storage media to store personal data unless the personal data on the media is encrypted.
- When picking up printing from any shared printer always check to make sure you only have the printed matter that you expect, and no third party's printing appears in the printing.
- Use confidential waste disposal for any papers containing personal data, do not place these into the ordinary waste; use a confidential waste service or have them shredded before placing them in the ordinary waste disposal.
- Do dispose of any materials containing personal data securely, whether the materials are paper based or electronic.
- When in a public place, e.g. a train or café, be careful as to who might be able to see the information on the screen of any device you are using when you have personal information on display. If necessary move location or change to a different task.
- Do ensure that your screen faces away from prying eyes if you are processing personal data, even if you are working in the office. Personal data should only be accessed and seen by those who need to see it.
- Do challenge unexpected visitors or employees accessing personal data.
- Do not leave personal data lying around, store it securely.
- When speaking on the phone in a public place, take care not to use the full names of individuals or other identifying information, as you do not know who may overhear the conversation. Instead use initials or just first names to preserve confidentiality.
- If taking down details or instructions from a customer in a public place when third parties may overhear, try to limit the information which may identify that person to others who may overhear in a similar way to if you were speaking on the telephone.
- Never act on instructions from someone unless you are absolutely sure of their identity and if you are unsure then take steps to determine their identity. This is particularly so where the instructions relate to information which may be sensitive or damaging if it got into the hands of a third party or where the instructions involve money, valuable goods or items or cannot easily be reversed.

- Do not transfer personal data to any third party without prior written consent of your line manager.
- Do notify your line manager or our Data Protection Officer immediately of any suspected security breaches or loss of personal data.
- If any personal data is lost, or any devices or materials containing any personal data are lost, report it immediately to our Data Protection Officer [For more details on this see our separate Data Breach Policy which applies to all Members regardless of their position or role in our organisation.

However you should always take a common sense approach, and if you see any areas of risk that you think are not addressed then please bring it to the attention of our Data Protection Officer.

11. Lawful basis for processing

The processing of personal data in Special Olympics GB is deemed necessary for legitimate interest reasons of the data controller or a third party (insurance company and international Special Olympics Programmes) Special Olympics GB processes Members' personal data in ways they would reasonably expect it to be processed where their membership with us is the compelling justification for the processing.

The processing may also be necessary for the performance of a contract with such Members or in order to take steps at the request of the Members.

12. Special category data

Special category data under the data protection laws is personal data relating to an individual's race, political opinions, health, religious or other beliefs, trade union records, sex life, biometric data and genetic data.

Under data protection laws this type of information is known as special category data and criminal records history becomes its own special category which is treated for some parts the same as special category data. Previously these types of personal data were referred to as sensitive personal data and some people may continue to use this term.

To lawfully process special categories of personal data i.e. health forms, we have confirmed that the processing is necessary to protect the vital interests and care, as well as assess the eligibility of the data subject to participate in Special Olympics. In addition, we will have explicit consent from the data subjects.

We would normally only expect to process special category personal data or criminal records history data usually in the context of our members/athletes/coaches/volunteers etc. for health and safety requirements and safeguarding checks, etc.

13. When do we process personal data?

Virtually anything we do with personal data is processing including collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction. So even just storage of personal data is a form of processing. We might process personal data using computers or manually by keeping paper records.

Examples of processing personal data might include:

- Using personal data to correspond with members;
- Holding personal data in our databases or documents; and
- Recording personal data in personnel or member files.

We process personal data every day for any number of purposes and in any number of ways. We must, therefore, comply at all times with the Data Protection Principles.

14. **Data protection principles and what you must do**

There are 6 data protection principles. Special Olympics GB is obligated to comply with these principles when we process personal data.

The principles are that personal data must be:

- processed lawfully, fairly and in a transparent manner and only if certain specified conditions are met;
- collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes ("**purpose limitation**");
- adequate and relevant, and limited to what is necessary to the purposes for which it is processed ("**data minimisation**");
- accurate and where necessary kept up to date;
- kept for no longer than is necessary for the purpose ("**storage limitation**"); and
- processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures ("**integrity and security**").

15. **Personal data must be processed fairly, lawfully and transparently.**

Special Olympics GB shall not process personal data obtained illegally (e.g. stolen), or obtained by misleading, pressurising or inducing an individual.

We shall inform an individual: who the data controller is (i.e. Special Olympics GB); the purpose for which personal data is to be processed; and any additional information that is necessary to ensure that the processing is fair and transparent.

In the majority of cases, it will be sufficient for the individual to have been provided with our privacy notice applicable to the category of individual to satisfy this requirement. This can be done by using our approved privacy notices. Therefore, accredited programmes must use approved standard privacy notices at all times.

16. **Personal data must be collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes ("purpose limitation").**

- We shall only process personal data for purpose for which it was collected e.g. if we have taken a member's details to forward information to them on our products and services, we will not pass those details on to a third party seeking to promote their services.
- If personal data is to be processed for another purpose, the individual must be informed of that purpose, and consent given by the individual.
- Again the purposes for which we collect and process personal data are set out in our standard privacy notices. This is another reason for accredited programmes make sure they always use our approved privacy notice.

17. **Personal data must be adequate and relevant, and limited to what is necessary to the purposes for which it is processed ("data minimisation")**

- Ensuring that the personal data can be used for the purposes for which it was collected, means collecting what we need to collect, but not more personal data than we need nor too little personal data.

- If we do not collect sufficient personal data to utilise it for its intended purpose, it shall be securely deleted or destroyed. If more personal data than is required has been collected, the unnecessary personal data will be securely deleted or destroyed.

18. **Personal data must be accurate and, where necessary, kept up to date.**

- We shall record personal data accurately. This is always important, but especially so where personal data is being entered into a database that may be reused on numerous occasions. Any mistakes or errors in the personal data will repeat themselves each time it is used.
- Wherever possible, we shall regularly confirm that personal data is correct and update databases accordingly (noting if personal data is incorrect and correcting it accordingly).
- Where we become aware that personal data is incorrect, then the personal data shall be corrected to remove the errors.

19. **Personal data must be kept for no longer than is necessary for the purpose ("storage limitation").**

- We shall delete data no longer required to fulfil the purposes for which it was originally collected.
- Retention period for data is set out in our standard privacy notice provided to the individual – period of membership with Special Olympics GB.

20. **Personal data must be processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures ("integrity and security")**

Any recorded information on athletes, volunteers, staff, and sponsors will be:

- Kept in locked cabinets
- Protected by the use of passwords if kept on a computer or other electronic devices
- Destroyed by shredding or other secure methods if no longer needed

Access to information on the main database is controlled by a password and only those needing access are given the password. Staff and volunteers should be careful about information that is displayed on their computer screen and make efforts to ensure that no unauthorised person can view the data when it is on display.

Foreign transfers of personal data

Personal data must not be transferred outside the European Economic Area (EEA) unless to a Special Olympics international programme which have an adequate level of protection for the rights of the data subject in relation to the processing of personal data.

Accredited programmes must not under any circumstances transfer any personal data outside of the EEA without our Data Protection Officer's prior written consent.

21. **Data subject rights**

Individuals have certain rights under data protection laws (**Rights**). These are:

- the right of access (also known as a data subject access request)
- the right to rectification

- the right to erasure (also known as the right to be forgotten)
- the right to restrict processing
- the right to data portability
- the right to object
- rights in relation to automated decision making and profiling.

The exercise of these Rights may be made in writing, including email, and also verbally and shall be responded to in writing by us (if we are the relevant data controller) without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. We shall inform the individual of any such extension within one month of receipt of the request, together with the reasons for the delay.

Where the data subject makes the request by electronic form means, any information is to be provided by electronic means where possible, unless otherwise requested by the individual.

If we receive the request from a third party (e.g. a legal advisor), we shall take steps to verify that the request was, in fact, instigated by the individual and that the third party is properly authorised to make the request. This will usually mean contacting the relevant individual directly to verify that the third party is properly authorised to make the request.

The exercise of these Rights may be restricted to safeguard:

- national security;
- defence;
- public security;
- the prevention and investigation of crimes;
- other objectives of general public interest, including economic interest;
- the protection of judicial proceedings;
- the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- a monitoring, inspection or regulatory function connected to the exercise of official authority in certain circumstances;
- the protection of the data subject or the rights and freedoms of others;
- the enforcement of civil law claims.

22. Notification and response procedure

If a Member receives a verbal request in relation to a Right, or you believe you have a verbal request for the exercise of a Right, you should:

- pass the call or person to your supervisor/manager if possible (unless you are a supervisor/manager). The supervisor/manager should make a written record of all relevant details and explain the procedure. If possible try to get the request confirmed in writing addressed to our Data Protection Officer. If it is not possible to transfer the individual over then make a written record of the request and contact details for individual making the request; and

- inform our Data Protection Officer of the request and pass them any written records relating to the request.

If a letter or fax exercising a Right is received by a member then you should:

- pass the letter to your supervisor/manager;
- the supervisor/manager must log the receipt of the letter with our Data Protection Officer and send a copy of it to them; and
- our Data Protection Officer will then respond to the individual on our behalf.

If an email exercising a Right is received by a member then you should:

- pass the email to their supervisor/manager;
- the supervisor/manager must log the receipt of the email with our Data Protection Officer and send a copy of it to them; and
- our Data Protection Officer will then respond to the individual on our behalf.

Our Data Protection Officer will co-ordinate our response which may include written material provided by us or external legal advisors. The action taken will depend upon the nature of the request and the Right. Our Data Protection Officer will write to the individual and explain the legal situation and whether we will comply with the request. A standard letter/email from our Data Protection Officer should suffice in most cases.

The manager/senior manager who receives the request will be responsible for ensuring that the relevant response is made within the time period required.

Our Data Protection Officer's reply will be validated by the relevant manager of the department producing the response. For more complex cases, the letter/email to be sent will be checked by external legal advisors.

23. Redactions

Where we are providing information to an individual where they have made a subject access request, they are only entitled to see their personal data. They are not entitled to see information which relates to other individuals or to other people, e.g. to a company.

In these cases we would redact, i.e. blank out in a permanent way, any information which is not the personal data of the individual making the subject access request.

24. Right to Erasure

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of their personal data where there is no compelling reason for its continued processing.

There are some specific circumstances where the right to erasure does not apply and we can refuse to deal with a request:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.

25. **Right to rectification**

An individual has the right to ask us to:

- correct inaccurate personal data;
- complete information if it is incomplete; and
- delete personal data which is irrelevant or no long required for our purposes.

26. **Right to Restrict Processing**

An individual is entitled to require us to stop or not begin processing their personal data. When processing is restricted, we are permitted to store their personal data, but not further process it except in the exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest. We can retain just enough information about the individual to ensure that the restriction is respected in future.

We will be required to restrict the processing of personal data in the following circumstances:

- where an individual contests the accuracy of the personal data, we should restrict the processing until we have verified the accuracy of the personal data;
- 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 our legitimate grounds override those of the individual;
- when processing is unlawful and the individual opposes erasure and requests restriction instead; and
- if we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

The individual does not have this right if the individual has entered into a contract with us and the processing is necessary for the fulfilment of that contract.

We will inform individuals when we decide to lift a restriction on processing (for example, if an individual contested our right to process their personal data on legitimate interest grounds and we subsequently found that our processing was justified on these grounds).

27. **The Right to Data Portability**

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. If the individual requests it, we may be required to transmit the data directly to another organisation if this is technically feasible. However, we are not required to adopt or maintain processing systems that are technically compatible with other organisations.

The right to data portability only applies:

- to personal data an individual has provided to a data controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

The information will be provided free of charge.

28. **Right to Object**

Individuals have the right to object to:

- processing based on legitimate interests;
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

If we process personal data on the basis of our legitimate interests, individuals must have an objection on “grounds relating to his or her particular situation”.

29. **Enforcement**

If an individual disagrees that we have properly complied with a Right or we fail to respond they may apply to a Court for an order or complain to the ICO in each case requiring us to properly perform the Right.

If the Court or the ICO agrees with the individual it can:

- order us to properly carry out the Right and what steps are needed to do this; and
- order us to notify third parties who we have passed the data onto of the Right;

A court can also award compensation to the individual for any damage they have suffered as a result of our non-compliance. The ICO can also impose a substantial civil fine upon us.

30. **Deleting personal data in the normal course**

We are only required to supply information in response to an exercise of Rights that was processed at the date of that request. However, we are allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of request in relation to a Right.

What will not amend or delete data because we do not want to supply it or because of the exercise of a Right.

31. **Queries**

If you have any queries about this Policy please contact either your line manager or our Data Protection Officer.

32. **Staff training and acceptance of responsibilities**

All staff that have access to personal data will be given copies of all relevant policies and procedures during their induction process, including the Data Protection Policy, Confidentiality Policy and the operational procedures for handling personal data. All staff will be expected to adhere to all these policies and procedures.
Data protection will be included in the induction training for all volunteers.
Special Olympics GB will provide opportunities for staff to explore data protection issues they may come across and procedural queries through training, team meetings, and supervisions.

Policy review

The policy will be reviewed in March every 2 years by the Chief Executive and approved by the Board of Trustees. It will also be reviewed in response to changes in relevant legislation, contractual arrangements, good practice or in response to an identified failing in its effectiveness.

Date this policy was approved by the Board of trustees: 14/05/2018

More information about your legal rights can be found on the Information Commissioner's website at https://ico.org.uk/for-the-public/.

Appendix A: Privacy statement

There are a number of grounds permitting Special Olympics GB to store and process our members' data for insurance cover purposes, Annual General Meeting notification, possible background checks and other purposes mentioned or referred to in the Data Protection Policies. This includes contractual necessity, explicit consent, protecting the member's vital interests and legislative interests of the Special Olympics GB or a third party. All information that we gather about you as an individual will be used to maintain our relationship with you and to provide you with information about our activities and for related purposes. The information will be held and processed by Special Olympics Great Britain strictly in accordance with the provisions of the data protection laws.

We will not, without your consent, supply your name and address to any third party except where (1) such a transfer is a necessary part of the activities that we undertake with an international Special Olympics programme or your local Special Olympics GB accredited programme, or (2) we are required to do so by the operation of the law or for the protection of your vital interests for or on a third party's legitimate interests. We will not share your information with third parties for their own marketing purposes.

Your data will be stored and processed for as long as you are a member of Special Olympics GB. As an individual, you have a right under the data protection laws to obtain information from us, including a description of the data that we hold on you. You also have other rights which are set out in the Data Protection Policy.

Please contact Special Olympics Great Britain, Corinthian House, 6-8 Great Eastern Street, London EC2A 3NT or info@sogb.org.uk with any queries.

Appendix B: Confidentiality statement for staff and volunteers

When working for Special Olympics GB, you will often need to have access to confidential information which may include, for example:

- Personal information about individuals who are supporters or otherwise involved in the activities organised by Special Olympics GB.
- Information about the internal business of Special Olympics GB.
- Personal information about colleagues working for Special Olympics GB.

Special Olympics GB is committed to keeping this information confidential, in order to protect people and Special Olympics GB itself. 'Confidential' means that all access to information must be on a need to know and properly authorised basis. You must use only the information you have been authorised to use, and for purposes that have been authorised. The information is required to be destroyed after its authorised use. You should also be aware that under the data protection laws, unauthorised access to data about individuals is a criminal offence.

You must assume that information is confidential unless you know that it is intended by Special Olympics GB to be made public. Passing information between an accredited programme and national office or between Special Olympics GB and a mailing house, or *vice versa* does not count as making it public, but passing information to another organisation does count.

You must also be particularly careful not to disclose confidential information to unauthorised people or cause a breach of security. In particular you must:

- not compromise or seek to evade security measures (including computer passwords);
- be particularly careful when sending information between the national office and accredited programmes;
- not gossip about or share in any unauthorised manner, confidential information, either with colleagues or people outside Special Olympics GB;
- not disclose information — especially over the telephone — unless you are sure that you know who you are disclosing it to, and that they are authorised to have it.
- Keep information securely as further outlined in data protection training

If you are in doubt about whether to disclose information or not, do not guess. Withhold the information while you check with an appropriate person whether the disclosure is appropriate.

Your confidentiality obligations continue to apply indefinitely after you have stopped working for Special Olympics GB.

I have read and understand the above statement. I accept my responsibilities regarding confidentiality.

Signed: Date: