**This template is designed to cover the policy issues relating to Data Protection that are pertinent to groups delivering sport and physical activity.**

**It has been designed to be adapted and amended to reflect the scope, activities, and procedures of your organisation. It also outlines the procedures that should be carried out to ensure compliance with the** [**General Data Protection Regulations**](https://www.lawdonut.co.uk/business/data-protection-and-it/data-protection/gdpr-your-data-protection-responsibilities) **legislation.**

**Items in green should be amended to reflect your group and your processes.**

**Once amended to reflect your activities it should be read by officers and coaches to ensure they understand their role and responsibilities in keeping everyone safe and keeping the organisation compliant.**

**There is a further document that accompanies this policy – The Privacy Notice which should be given to each of your data subjects – officers, staff, volunteers, members, and child members’ parents / carers in order to secure understanding of GDPR and to gain consent for processing their personal data**

**There is also a procedure checklist to assist you in identifying whether you have the appropriate processes and procedures in place**

**Disclaimer: Please remember that our resources reflect core governance principles and good practice but do not constitute legal advice.**

**XX Data Protection Policy**

1. **Legal requirement**

[General Data Protection Regulations](https://www.lawdonut.co.uk/business/data-protection-and-it/data-protection/gdpr-your-data-protection-responsibilities) (GDPR) 2018 applies to every organisation that collects, stores, and uses personal data relating to members, staff, or other individuals.

This policy has been developed to help XX comply with the [GDPR requirements](https://www.lawdonut.co.uk/business/data-protection-and-it/data-protection/gdpr-your-data-protection-responsibilities) by setting out clear procedures to be followed by officers, staff and volunteers; to ensure everyone involved with XX understands why data protection is important and the requirements for collecting, working with, and storing data. This should be read in conjunction with the XX Privacy Notice

GDPR compliance is necessary as the XX acts as a data controller. For example, we hold personal data on our officers, volunteers, staff, and members (“individuals”).

The lawful basis on which XX processes data is

a) Consent: the individual has given clear consent for us to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract we have with the individual.

(c) Legal requirement: the processing is necessary to comply with Health and Safety regulation and to safeguard the individual

1. Accountability for data protection

XX takes its responsibility for data protection seriously and *officers, staff and volunteers must have access to and understand this policy.* XX has appointed officers specifically to be accountable for the maintenance and implementation of this policy

**Data protection Lead**:

Number: E-mail:

**Data protection Deputy Lead**:

Number: E-mail

1. Key principles of data protection underpinning this policy:
2. Personal data must be processed lawfully, fairly, and transparently
3. Data should only be collected and processed for a specific, legitimate purpose and not used any way that is not compatible with that purpose
4. Only that data that is necessary in relation to the specific requirement should be collected and processed
5. Personal data should be accurate and, where necessary, kept up to date
6. Personal data should identify the data subjects to enable accurate record keeping so that it is kept for no longer than is necessary
7. Appropriate security measures should be put in place (such as encryption, passwords, and securely locked cabinets) to protect against unlawful or unauthorised processing, and against loss, destruction, or damage.
8. Definition of personal data

**Personal data** are any **information** which is related to an identified or identifiable natural person. These comprise:

1. All individuals’ records, membership databases, correspondence, reports
2. Technical data such as IP addresses, smartphone device IDs or location information if it can be linked to an individual.
3. Records maintained in a manual filing system, as well as computerised records.

Some personal data is particularly **sensitive.** XX may collect such data for reporting on activity and project outcomes etc. Sensitive data includes:

1. information on racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, and information on sex life or sexual orientation or about an individual's criminal convictions.
2. Genetic or biometric data are also sensitive data.
3. Consent

XX has developed a Privacy Notice to advise individuals of our data protection policy principles and their rights, as personal data must be processed lawfully, fairly, and transparently.

A copy of the privacy notice will be given to each individual when they join

Consent will be sought from all individuals for whom XX holds personal data within 7 days of joining, and a record maintained of this consent

A consent forms are included in the appendices of the privacy notice, and, as special rules apply for children, a consent form is included to secure the consent of the parent or carer.

*We will keep clear records where consent has been requested.*

1. The type of personal data used

We collect, process, and store the following information, about individuals

* **Identity Data**: title, name, address, home or work phone numbers, home or work email address, Job title and position,
* **Financial Data**: bank account and card payment details, invoicing details
* **Special Category Data:** health, medical data, learning needs, race, religion
* **Transaction Data:** Payments for services individuals have brought from us, or payments we have made to you.
* **Technical Data:** which refers to data which can be used to identify individuals indirectly such as IP address, cookie identifier, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices used to access our Website
* **Profile and Usage Data:** this may include feedback and survey responses, enquires submitted by individuals. This may also include how individuals use our website, products, services and booking system
* **Marketing Data:** ways in which we keep individuals up to date with communications from us to them. Individuals can tell us which way they prefer us to contact them by email, text, or post.

1. How we get the personal information and why we have it

Most of the personal information we process is provided to us directly by individuals for one of the following reasons:

* So we can tell individuals about our services, and so we can meet our commitments to them
* So we can keep individuals involved in our services safe. Some of the information we obtain i.e. medical, health, behavioural and learning needs will help us meet our members’ needs
* So we can notify individuals of any changes to our services
* If you are an existing member, we may contact individuals about similar services we provide which may be of interest to them
* So XX can provide updates in the form of *newsletters, emails, texts, or social media posts*
* Some of the services we run we are obligated to pass data onto sport governing bodies or funders. This may include the xxxxxxxxx
* For marketing purposes, we may collect individuals’ data for internal use,
* From time to time we may ask individuals to complete surveys and or to give us feedback on our activities, this helps us to improve our services.
* We also collect this information and data so we can show what impact our services are having in our members’ lives, sometimes we are obligated to do this from our funders, but other times we do it to attract new funding. We may be asked to provide named case studies, for which we would always ask for individual consent

1. Individual rights

You (in common with other data subjects) have the following rights in relation to your personal information:

* to be informed about how, why and on what basis that information is processed—see the XX data protection privacy notice;
* to obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request—see the XX's subject access request policy;
* to have data corrected if it is inaccurate or incomplete;
* to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');
* to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal information but you require the data to establish, exercise or defend a legal claim; and
* to restrict the processing of personal information temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether the organisation's legitimate grounds override your interests).

If you wish to exercise any of the rights above, please contact Name - contact.

1. Individual obligations

Individuals are responsible for helping the XX keep their personal information up to date. You should let XXX know if the information you have provided to XX changes, for example if you move house or change details of the bank or building society account to which you are paid. Alternatively, you can update your own personal information on a secure basis via the XX’s intranet.

You may have access to the personal information of other members of staff, suppliers and customers of XX in the course of your employment or engagement. If so, XX expects you to help meet its data protection obligations to those individuals. For example, you should be aware that they may also enjoy the rights set out in paragraph above.

If you have access to personal information, you must:

* only access the personal information that you have authority to access, and only for authorised purposes;
* only allow other XX staff to access personal information if they have appropriate authorisation;
* only allow individuals who are not XX staff to access personal information if you have specific authority to do so from the HR Department;
* keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in the XX's information security policy);
* not remove personal information, or devices containing personal information (or which can be used to access it), from XX's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and
* not store personal information on local drives or on personal devices that are used for work purposes and comply with XX's BYOD policy.

You should contact HR Department if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

* processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions being met;
* any data breach as set out below;
* access to personal information without the proper authorisation;
* personal information not kept or deleted securely;
* removal of personal information, or devices containing personal information (or which can be used to access it), from XX's premises without appropriate security measures being in place;
* any other breach of this policy or of any of the data protection principles set out above.

1. Data Management
2. **Data Collection** - As data should only be collected and processed for the specific, legitimate purposes outlined above and not used any way that is not compatible with that purpose, when collecting personal information XX will:
3. *We collect the minimum of personal data*
4. *Not collect extra information just because it might be helpful later.*
5. *Will not keep data longer than we need to.*
6. **Data Maintenance**

Personal data should be accurate and, where necessary, kept up to date. To do this, the data protection lead will ensure:

1. *Appropriate data is collected when individuals join* XX
2. *The accuracy and propriety of data held is checked annually and amendments made within 7 days to correct any errors and omissions, or to delete inappropriately held data*
3. *A review of data policy and procedures is carried out in the event of a serious data incident e.g. loss of data corruption of data, inappropriate disclosure of data.*
4. *Personal data is be deleted within 12 months of members leaving.*
5. *Personnel records are maintained in line with the requirements of statutory agencies e.g. HMRC*
6. *We keep clear records of what action we have taken, and what steps taken to protect the data*.

Personal data will identify the data subjects to enable accurate record keeping

1. **Data security**

Data security is of paramount importance in XX. To ensure that personal data held is secure we have:

* *Assigned someone to take responsibility for GDPR as data protection lead and*
  + *provided them with the resources and training to understand the organisational, legal, and technical issues involved,*
  + *required them to carry out annual review of the propriety of data held*
  + *required them to report annually on compliance with GDPR directly to senior management or after any significant data incident*.
* *Assigned a deputy to support the data protection lead, who has appropriate knowledge and training*
* *Secured training and information for all officers, staff, and volunteers to make sure they are aware of the importance of data protection and understand the procedures they must follow.*
* *Established appropriate security measures, to protect against unlawful or unauthorised processing, and against loss, destruction, or damage including:*
* *technical security - such encryption, passwords, firewalls and anti-virus software*
* *Physical security – locked premises, alarms, security cameras securely locked cabinets to protect against theft or loss of data, either on computer systems or paper-based.*
* *Locking away laptops and smartphones at home or out of view in vehicles and data on employees' own systems (e.g. for homeworking)*
* *Making sure officers, staff and volunteers understand and follow security procedures.*
* *Maintained clear records of what action we have taken in respect of data security, and what steps taken to protect the data.*
* *Reviewed the policy and privacy notice annually and keep clear records of what action we have taken, and what steps taken to protect the data.*

1. **Data protection impact assessments (DPIAs)**

Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where XX is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

* whether the processing is necessary and proportionate in relation to its purpose;
* the risks to individuals; and
* what measures can be put in place to address those risks and protect personal information.

Before any new form of technology is introduced, the manager responsible should therefore contact HR Department in order that a DPIA can be carried out.

During any DPIA, XX will seek the advice of HR Department and the views of a representative group of employees and any other relevant stakeholders.

1. **Documentation and records**

XX will keep written records of processing activities which are high risk, i.e. which may result in a risk to individuals' rights and freedoms or involve sensitive personal information or criminal records information, including:

* *the name and details of XX (and where applicable, of other controllers, XX’s representative and DPO);*
* *the purposes of the processing;*
* *a description of the categories of individuals and categories of personal data;*
* *categories of recipients of personal data;*
* *where possible, retention schedules; and*
* *where possible, a description of technical and organisational security measures.*

*As part of our record of processing activities we document, or link to documentation, on:*

* *information required for privacy notices;*
* *records of consent;*
* *controller-processor contracts;*
* *the location of personal information;*
* *DPIAs; and*
* *records of data breaches.*

*If we process sensitive personal information or criminal records information, we will keep written records of:*

* *the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;*
* *the lawful basis for our processing; and*
* *whether we retain and erase the personal information in accordance with our policy document and, if not, the reasons for not following our policy.*

*XX will conduct regular reviews of the personal information we process and update our documentation accordingly. This may include:*

* *carrying out information audits to find out what personal information the holds;*
* *distributing questionnaires and talking to staff across XX to get a more complete picture of our processing activities; and*
* *reviewing our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.*

We document our processing activities in electronic form so we can add, remove and amend information easily.

1. **In the event of a security incident**

*A data breach may take many different forms, for example:*

* *loss or theft of data or equipment on which personal information is stored;*
* *unauthorised access to or use of personal information either by a member of staff or third party;*
* *loss of data resulting from an equipment or systems (including hardware and software) failure;*
* *human error, such as accidental deletion or alteration of data;*
* *unforeseen circumstances, such as a fire or flood;*
* *deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and*
* *'blagging' offences, where information is obtained by deceiving the organisation which holds it.*

*XX will:*

* *make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and*
* *notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.*

*XX will report any data breach that is likely to harm individuals to the Information Commissioners Office - for example, because personal data has been put at risk,*

* *within 72 hours of becoming aware of it,*
* *providing information on what has happened, including what data and individuals are at risk, and*
* *what we are doing about it.*

*We will inform individuals*

* *if they have been put at high risk for example, if a hacker may have gained access to credit card details or be able to commit identity fraud.*
* *without undue delay and give clear information on what has happened.*

We do not need to report the loss of a securely encrypted USB containing personal data or where the breach only relates to the disclosure of the names and addresses of individuals as it is unlikely to be high risk, if these are already publicly available

1. International transfers

The Employer will not transfer personal information outside the European Economic Area (EEA), which comprises the countries in the European Union and Iceland, Liechtenstein and Norway.

OR

*XX* may transfer personal information outside the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein and Norway) to insert name of country on the basis that that country, territory or organisation is designated as having an adequate level of protection OR that the organisation receiving the information has provided adequate safeguards by way of binding corporate rules OR standard data protection clauses OR of compliance with an approved code of conduct.

1. Further guidance and information

Find [guidance for business](https://ico.org.uk/for-organisations/) from the Information Commissioner's Office (0303 123 1113).

The helpline (0303 123 1113). is a dedicated small business advice line offering help with GDPR, data protection, and other legislation they regulate.

I have read and understood this policy and agree to abide by its terms.

Signed....................................................................................................

This Policy will be reviewed by xx.xx 21