Data Protection Policy

Organisation Name: Kilkenny Recreation & Sports Partnership

Policy Approved by KRSP Board on 13/12/2018

Version Number	Review Date	Nature of Revisions
1.0	30 April 2018	

1. Introduction

1.1. The General Data Protection Regulation

The General Data Protection Regulation 2016 [EC/2016/679] replaces the EU Data Protection Directive [95/46/EC] and supersedes the laws of individual European Union member states that were developed in compliance with Data Protection Directive [95/46/EC]. The purpose of the General Data Protection Regulation (hereafter referred to as the "GDPR") is to protect the "rights and freedoms" of natural persons (i.e. living persons) and to ensure that personal data is not processed without their knowledge, and wherever possible, that it is processed with their consent.

1.2 Definitions

1.2.1 Material Scope – GDPR Article 2

The GDPR applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

1.2.2 Territorial Scope – GDPR Article 3

The GDPR applies to the processing of personal data in the context of the activities of an establishment of a Controller or a Processor in the Union, regardless of whether the processing takes place in the Union or not.

The GDPR applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

- the monitoring of their behaviour as far as their behaviour takes place within the Union.

1.2.3 Definitions – GDPR Article 4

For the purposes of the GDPR, the following definitions apply:

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future.

Filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Data controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Third party means 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.

Personal data breach means 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.

Supervisory Authority means an independent public authority which is established by a Member State pursuant to Article 51.

1.3 Data Protection Acts

The data protection acts to which Kilkenny Recreation & Sports Partnership (KRSP) is subject are the Data Protection Acts of 1988 and 2003 together with the Data Protection Act 2018 which gives further effect under Irish law to the GDPR and enactment of the Law Enforcement Directive [EC/2016/680].

1.4 Company Obligations

In undertaking the business and activities of KRSP (hereafter referred to as "The Company"), we create, gather, store and process personal data on a variety of data subjects including participants, service providers, beneficiaries, staff, Board members, volunteers, donors, suppliers and members of the public. The Company's use of personal data ranges from enquiries, CCTV footage, financial transactions with participants, service providers and suppliers through to the processing of participant and beneficiary data throughout their journey and interactions with The Company. As The Company processes the personal data of participants, service providers, beneficiaries, staff, Board members, volunteers, donors, suppliers and members of the public, it is defined as a Data Controller for the purposes of the GDPR.

The GDPR applies to all data relating to, and descriptive of, living individuals defined in the GDPR as personal data. Individuals are referred to as 'data subjects'.

Some of the data that The Company creates, collects and processes may be sensitive data i.e. data concerning a data subject's racial or ethnic origin, political opinions, religious beliefs, physical or mental health, sexual life, genetic data or trade union membership.

Data protection is an important part of The Company's overall information security arrangements. All information must be handled safely and securely in accordance with The

Company's policies and procedures. In addition, some data sets are subject to external regulation/legislation and it is important that staff/Board members/service providers/volunteers recognise both categories when handling The Company's information and data.

The GDPR and data protection acts place obligations on The Company and the way it handles personal data. In turn, the staff/Board member/service providers/volunteers in The Company have responsibilities to ensure that personal data is processed fairly, lawfully and in a transparent manner. Staff/service providers/volunteers also have responsibilities to ensure that personal data is processed securely. The Company should only process data if we have a valid condition of processing (e.g. consent from the data subject or a service agreement with the data subject) and we have provided information to data subjects about how and why we are processing their information (i.e. privacy notice). There are restrictions on what The Company is allowed to do with personal data such as passing personal information on to third parties, transferring information outside the European Economic Area or using it for the purposes of fundraising or direct marketing.

2. Purpose of Policy

This Data Protection Policy sets out the responsibilities of The Company, its staff, Board members, service providers, volunteers, contractors, agents and third parties associated with The Company with respect to compliance with the GDPR and data protection acts. This policy and its associated policies and procedures, forms the framework from which staff, Board members, service providers, volunteers, contractors and associated third parties should operate to ensure compliance with the GDPR and data protection legislation.

3. Scope

The policy applies to all staff, Board members, service providers, volunteers, contractors, agents and third parties associated with The Company, and all items of personal data that are created, collected, stored and/or processed through any activity of The Company, across all its services and activities. Unless specifically stated otherwise, personal data and sensitive data will be referred to equally as personal data in this policy.

4. Data Protection Principles

The Company is required to adhere to the data protection principles as set out in Article 5 of the GDPR, meaning that information must be collected and used fairly, stored safely and not

shared with any other person unlawfully. The data protection principles are set out in sections 4.1 to 4.7 inclusive.

4.1 Lawful, fair and transparent processing

Data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

The Company will ensure that at least one of the lawful basis for processing listed below will be met whenever data processing takes place.

- Processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract.

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.

- Processing is necessary for compliance with a legal obligation.

- Processing is necessary to protect someone's vital interests.

- Consent has been obtained from the data subject for the processing of his or her personal data for one or more specific purposes.

- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject, which require protection of personal data, in particular where the data subject is a child.

In circumstances where The Company processes sensitive data (i.e. special categories of data), extra more stringent conditions will be met in accordance with Article 9 of the GDPR.

In circumstances where The Company relies upon consent from the data subject as the basis for data processing, consent must be freely given, informed and unambiguous and indicated through the provision of a clear statement or other clear affirmative action, signifying the data subject agrees to the processing of his or her information.

In the interests of fairness and transparency, The Company will make the data subject aware of the following information at the time the data is collected directly:

- Name of the Data Controller and name and contact details of the Data Protection Liaison Contact in The Company

- Purpose and legal basis for processing including an explanation of the legitimate interest of The Company if legitimate interest is the basis for personal data processing.

- The data subject's rights to request access, rectification, restriction, withdraw consent, complain to the Data Protection Commissioner's office.

- Recipients of the personal data.

- Data retention periods or criteria used to calculate data retention period.

- Legal basis for intended international transfer of personal data to a third country or organisation.

In circumstances where The Company does not collect personal data directly from the data subject, the source of the data, in addition to the information listed above, will be provided to the data subject within 30 days of obtaining the data. Information will not be provided to the data subject if it will require disproportionate effort or seriously impair the purpose for processing.

A fair processing notice will be placed in a visible position where activity is recorded by The Company on CCTV or video.

The data subject's personal data will not be disclosed to a third party other than to a third party contracted to The Company and engaged in processing activities on its behalf.

4.2 Data collected for specified, explicit and legitimate purposes

Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes subject to appropriate data privacy safeguards.

The data subject will be informed of the purposes for which The Company processes data at the time the data is collected or within 30 days if obtained by a third party. Data will not be processed further in a way that is incompatible with these purposes by The Company unless the consent of the data subject has been obtained, or processing is for archiving purposes in the public interest or scientific or historical research, or statistical purposes and appropriate data safeguards are in place and there is no risk of breaching the privacy of the data subject.

4.3 Data should be adequate, relevant and limited

The Company will ensure that data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is being processed for the specific purposes informed to data subjects.

4.4 Data should be accurate

The Company will ensure that data collected will be kept accurate and, where necessary, kept up to date; and every reasonable step 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.

4.5 Identification of data subjects for no longer than is necessary

The Company will ensure that 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

Statutory data retention periods may exist in relation to types of data being processed e.g. health and safety, employment regulations. Where statutory data retention periods are not specified, data retention periods will be set to limit the storage of data for a period no longer than is necessary for which the data is processed.

Once the data retention has expired, the data will be deleted/destroyed in the absence of a new lawful basis for processing to retain it. The Company may store the data for longer periods for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes ensuring appropriate safeguards are in place i.e. data anonymisation.

4.6 Secure processing

Data collected and processed is kept secure 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. The Company will consider the nature of the data, the costs associated with implementing measures and technological developments when determining security measures. The Company shall keep under review the associated risks of proposed data processing and the impact on an individual's privacy in holding personal data about them.

4.7 Accountability

Article 5(2) states that data controllers are responsible for and must be able to demonstrate compliance with the data protection principles.

In demonstrating compliance with the GDPR, The Company:

- Keeps an internal record of all data processing activities in accordance with Article 30 – "Records of Processing Activities." These records will be disclosed to the Supervisory Authority i.e. Data Protection Commissioner's Office upon request.

  When the Company is acting as Data Controller this record (referred to internally as a Data Matrix) will contain the following:

  - List of personal data being processed
  - Categories of data subjects
  - Source of personal data
  - Processing activities and location where data is stored
  - Categories of recipients (i.e. with whom data will be shared)
  - Data retention period for each type of personal data being processed
  - Methods for deleting data
  - International data transfers and safeguards (measures) in place to ensure transfers are lawful
  - Details of security measures implemented in respect of processed data
  - Contact details for the Data Controller and Data Protection Liasion Contact

  When The Company is acting as Data Processor the record (Data Matrix) will contain the following:

  - Categories of processing carried out on behalf of the Data Controller
  - International data transfers and safeguards (measures) in place to ensure transfers are lawful
  - Name of the Data Controller and contact details including those of the Data Protection Liasion Contact

- The Company maintains a Data Protection Management File which contains all data protection policies, procedures and training records.

- The Company will appoint a Data Protection Officer if required in circumstances where:

  - The Company regularly and systematically engages in large scale processing of personal data; or
  - The Company engages in large scale processing of sensitive personal data.

- The Company ensures that data protection by design is addressed both at the planning stage and throughout the lifecycle of data processing activity.

- The Company implements data protection by default processing only the personal data that is necessary and selecting the most data protective settings by default.

- If a high degree of risk to the rights and freedoms of data subjects may arise from the processing activities of The Company, a Data Protection Impact Assessment will be conducted.

5. Subject Access Requests and Data Subject Rights

The GDPR and data protection acts give individuals the right to access information held about them by The Company. The Company must respond to all requests for personal information and will normally provide information free of charge. Individuals may request to see any personal information The Company holds about them including copies of email correspondence. The Company will manage requests in a timely manner within the timelines stipulated by the GDPR and Data Protection Act 2018.

Where a data subject makes a formal request to The Company with respect to the information held by The Company, such a request gives rise to the following access rights under the GDPR and in accordance with the Data Protection Act 2018:

- The right to be informed
- The right of access
- The right to erasure
- The right of rectification
- The right to restrict processing
- The right to object
- The right to data portability
- The right to withdraw consent for data processing
- Rights with respect to data profiling and automated decision-making

Where necessary, subject access requests will be forwarded to The Company's designated Data Protection Liasion Contact in a timely manner and processed efficiently and in accordance with The Company's Subject Access Request procedure.

6. Sharing Data with Third Parties

Data subject's information will not be shared with third parties for marketing or fundraising purposes.

Data will only be shared with third parties for the purposes set out below:

Third Party Description	Purpose for Sharing Data
Sub-contractors	To help The Company to run our business in an effective manner under our terms and conditions of contract with data subjects
Cloud Service Providers	To store information legitimately held by The Company for business purposes
IT Back-up Providers	To store information legitimately held by The Company for business purposes
IT Service Providers	To store information legitimately held by The Company for business purposes and for IT security and services
Email Service Providers	To help The Company to run our business in an effective manner for legitimate business purposes
Internal Customer Databases	To run internal customer databases in an effective manner under The Company's terms and conditions of contract with data subjects

7. Photographs and Video

Images of staff, Board members, participants, service providers and beneficiaries may be captured at appropriate times as part of its service delivery activities. Unless prior consent has been obtained from staff, Board members, participants, service providers and beneficiaries, The Company will not use such images for publication or communication to external sources. It is The Company's policy that external parties (including family members and friends associated with staff, beneficiaries and clients) may not capture images of staff, Board members, participants, service providers and beneficiaries attending The Company's events and activities without prior consent.

8. Organisational Measures

The Company shall ensure that appropriate organisational measures are taken with respect to personal data collection, personal data storage and personal data processing. These measures include:

All staff, Board members, service providers, volunteers, contractors, agents and third parties working on behalf of The Company will be made fully aware of their individual responsibilities and The Company's responsibilities under the GDPR and be provided with an opportunity to read The Company's Data Protection Policy.

All staff, Board members, service providers, volunteers, contractors, agents and third parties working on behalf of The Company will have access to personal data held by The Company, if they need access to and use of personal data to carry out their assigned duties.

All staff, Board members, service providers, volunteers, contractors, agents and third parties working on behalf of The Company will be appropriately trained in the handling of personal data and are required to comply with any and all of The Company's guidelines and instructions for the processing of personal data.

All contractors, agents and third parties working on behalf of The Company are bound by the principles of the GDPR and this Data Protection Policy by contract and must ensure that all of their employees and associates, who are involved in the processing of personal data, are held to the same conditions as the staff, Board members, service providers and volunteers of The Company arising out of the GDPR and this Data Protection Policy.

The performance of all staff, Board members, service providers, volunteers, contractors, agents and third parties working on behalf of The Company handling personal data will be reviewed and evaluated regularly.

The Company recognises that the secure disposal and erasure of redundant personal data is an important element to compliance with the GDPR. All personal data held in any form of media shall only be passed to a data disposal partner with demonstrated competence in providing secure disposal services.

Personal data collection, storage and processing methods will be reviewed and evaluated regularly.

[Please list the specific technical and organisational measures you are taking to safeguard personal data during processing and storage. Alternatively, put these measures in an Information Security Policy and ask people to read the policy as it forms part of your data protection framework.]

9. Transferring Personal Data outside of the European Economic Area

The transfer of personal data to a country outside of the European Economic Area will only take place if one or more of the following applies:

- The country has been determined by the European Commission to have an adequate level of protection for personal data.
- The country or international organisation provide appropriate safeguards in the form of binding corporate rules, a legally binding agreement between public authorities or bodies, or complies with an approved code of conduct approved by a supervisory authority.
- The transfer is necessary to protect the vital interests of the data subject(s).
- The transfer is made with the informed consent of the data subject(s).
- The transfer is necessary for the conduct of legal claims.
- The transfer is made from a register that is publically accessible under Irish or EU law.

10. Data Breach Notification

The Company treats data breaches very seriously. Any staff, Board member, service provider, volunteer, contractor, agent or third party who becomes aware of a likely data breach and fails to notify the Data Protection Liaison Contact, may be subject to the Company's disciplinary procedures depending on the severity of the breach.

The Company Data Breach Notification Procedure with respect to staff, Board members, service providers, volunteers and communication with the Data Protection Commissioner is contained in a separate document. Please see relevant document for further details.

11. Policy Implementation

The Company ensures that any individual or entity that processes personal data on its behalf does so in a GDPR compliant manner. Failure of a data processor to process and manage The Company's personal data in a GDPR compliant manner will be viewed as a breach of contract. Failure of staff, Board members, service providers and volunteers of The Company to process and manage personal data in compliance with this Data Protection Policy may result in disciplinary proceedings.

12. Data Protection Liaison Contact

The contact details for The Company's designated Data Protection Liaison is:

Name:	Nicola Keeshan
Company Postal Address:	John's Green House, John's Green, Kilkenny
Telephone:	056 7794991
Email:	nicola@krsp.ie