Rugby League Ireland Data Protection Policy - December 2025

Initial Approval Date: March 2021					
Revision and Approval History					
Version	Revised By	Revision Date	Approved By	Approval Date	Comments
1	Adam Cox	March 2021	Board		
2	Craig Best	December 2025	Board	January 2026	All appropriate revisions made to policy from law changes and amendments post 2021.

Data Protection Policy

Everyone has rights regarding how their personal information is handled. During the course of our activities, Rugby League Ireland will collect, store and process personal information and we recognise the need to treat it in an appropriate and lawful manner.

Under the legislation, Rugby League Ireland is known as a "Data Controller" of all personal information used in our business.

Key words in relation to Data Protection

The following are key terms that are commonly used in relation to data protection:

Personal Data is data that relates to a living individual who can be identified from that data (or from that data and other information in or likely to come into our possession). That living individual might be an employee, member, coach, athlete, supplier, contractor or contact, and that personal data might be written, oral or visual (e.g. CCTV).

Identifiable means that the individual can be distinguished from a group of individuals (although the name of that individual need not be ascertainable). The data might identify an individual on its own (e.g. a name or video footage) or might do if taken together with other information available to or obtainable by us (e.g. a job title and company name). More details on this can be found in part 2 of this Policy.

Data Subject is the living individual to whom the relevant personal data relates.

Processing is widely defined under the data protection laws and generally any action taken by us in respect of personal data will fall under the definition, including for example collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction of personal data, including CCTV images.

Data Controller is the person who decides how personal data is used, for example we will always be a data controller in respect of personal data relating to our employees.

Data Processor is a person who processes personal data on behalf of a data controller and only processes that personal data in accordance with instructions from the data controller, for example an outsourced payroll provider will be a data processor.

Contents

1. Introduction

This Policy sets out the obligations of Rugby League Ireland ("**the Company**") regarding data protection and the rights of different type(s) of data subjects, e.g. customers, business contacts etc. ("**data subjects**") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("**GDPR**").

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 GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "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.

To expand further, data will relate to an individual and therefore be their personal data if it:

- identifies the individual. For instance, names, addresses, telephone numbers and email addresses;
- its content is about the individual personally. For instance, medical records, credit history, a recording of their actions, or contact details;
- relates to property of the individual, for example their home, their car or other possessions;
- it could be processed to learn, record or decide something about the individual (or this is a consequence of processing). For instance, if you are able to link the data to the individual to tell you something about them, this will relate to the individual (e.g. salary details for a post where there is only one named individual in that post, or a telephone bill for the occupier of a property where there is only one occupant);
- is biographical in a significant sense, that is it does more than record the individual's connection with or involvement in a matter or event which has no personal connotations for them. For instance, if an individual's name appears on a list of attendees of an organisation meeting this may not relate to the individual and may be more likely to relate to the company they represent;
- has the individual as its focus, that is the information relates to the individual personally rather than to some other person or a transaction or event he was involved in. For instance, if a work meeting is to discuss the individual's performance this is likely to relate to the individual;
- affects the individual's privacy, whether in their personal, family, organisation or professional capacity, for instance, email address or location and work email addresses can also be personal data;
- is an expression of opinion about the individual e.g. records stored in the course of a coaching assessment or details regarding a participant's performance; or
- is an indication of our (or any other person's) intentions towards the individual (e.g. how a complaint by that individual will be dealt with).

Information about companies or other legal persons who are not living individuals is not personal data. However, information about directors, shareholders, officers and employees, and about sole traders or partners, is often personal data, so business related information can often be personal data.

Examples of information likely to constitute personal data:

- Unique names;
- Names together with email addresses or other contact details;
- Job title and employer (if there is only one person in the position);
- Video - and photographic images;
- Information about individuals obtained as a result of Safeguarding checks;
- Medical and disability information;
- Member profile information (e.g. marketing preferences); and
- Financial information and accounts (e.g. information about expenses and benefits entitlements, income and expenditure).

Examples of information unlikely to constitute personal data:

- Reference to the individual's name in a document that contains no other personal data about that them (e.g. including the individual in a list of attendees of a meeting where the individual attended in an official capacity on behalf of a company); and
- Where the individual's name appears in an email that has been sent to or copied to them, but where the content is not about him or her (e.g. emails sent to the individual about an organisation's dealings).

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.

This Policy details the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

Rugby League Ireland requires each employee, volunteer, manager, contractor or consultant to fully comply with this policy. Any breach of this policy will be taken seriously and may result in disciplinary action, or termination of contract (employment or with a contractor/consultant).

2. The Data Protection Principles and Main Obligations

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, for example you will have received one of these from us as one of our employees;
- 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 employee/volunteer/consultant/contractor 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 Ireland is enforced by the Data Protection Commissioner's Office and they are the regulator for Data Protection in Ireland. They have extensive powers, including the ability to impose civil fines of up to Euros €20 million. Also the Data Protection laws can be enforced in the courts and the courts have the power to award compensation to individuals.

Data Protection Principles

The Data Protection laws set out six 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").

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 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 Breach Policy which applies to all employees regardless of their position or role in our organisation.

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.

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.

What does this mean?

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.

Areas and activities particularly affected by Data Protection laws include Human Resources, payroll, security, member/customer support, sales, data inputting, marketing and 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.

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 safe or the hotel staff 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, place them in a bin or skip etc., and either 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 consent of your line manager or our Data Protection Officer.

- Do notify 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 employees 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.

Queries

If you have any queries about this Policy please contact either your line manager or our Data Protection Office – secretary@rli.ie

3. The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

- The right to be informed (Part 12)
- The right of access (Part 13)
- The right to rectification (Part 14)
- The right to erasure (also known as the 'right to be forgotten') (Part 15)
- The right to restrict processing (Part 16)
- The right to data portability (Part 17)
- The right to object (Part 18) and
- Rights with respect to automated decision-making and profiling (Parts 19 and 20).

4. Lawful, Fair and Transparent Data Processing

The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:

- The data subject has given consent to the processing of their personal data for one or more specific purposes
- The 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 with them
- The processing is necessary for compliance with a legal obligation to which the data controller is subject
- The processing is necessary to protect the vital interests of the data subject or of another natural person
- The 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 or
- The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by 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.

If the personal data in question is “special category data” (also known as “sensitive personal data”) (for example, data concerning the data subject’s race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:

- The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so)
- The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject)
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects
- The processing relates to personal data which is clearly made public by the data subject
- The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity
- The processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject
- The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR
- The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy) or
- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

- Rugby League Ireland relies on a range of lawful bases for processing personal data, including contractual necessity (e.g. membership administration), legal obligation (e.g. safeguarding and governance requirements), and legitimate interests (e.g. competition administration and communications).

- Consent is not relied upon where another lawful basis is more appropriate. Special category data, including health and safeguarding information, is processed only where necessary and with appropriate safeguards in place.

Children's Personal Data

Rugby League Ireland recognises that children merit specific protection with regard to their personal data, as they may be less aware of risks, consequences, and safeguards.

Personal data relating to children will be processed fairly, lawfully, and transparently, and only where necessary for the administration, safeguarding, and development of rugby league activities.

Where consent is relied upon as a lawful basis, it will be obtained from a parent or legal guardian in accordance with applicable law. Information provided to children and parents will be age-appropriate, clear, and easily understood.

Children's personal data will not be used for marketing or profiling purposes and will be retained only for as long as necessary in line with Rugby League Ireland's data retention practices.

5. Specified, Explicit and Legitimate Purposes

The Company collects and processes the personal data set out in Part 21 of this Policy. This includes:

- Personal data collected directly from data subjects
- Personal data obtained from third parties
- The Company only collects, processes, and holds personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the GDPR)
- Data subjects are kept informed at all times of the purpose or purposes for which the Company uses their personal data. Please refer to Part 12 for more information on keeping data subjects informed.

6. Adequate, Relevant and Limited Data Processing

The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 5, above, and as set out in Part 21, below.

7. Accuracy of Data and Keeping Data Up-to-Date

The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 14, below

The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8. Data Retention

The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed

When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay

For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Policy.

9. Secure Processing

The Company shall ensure that all personal data collected, held and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 22 to 27 of this Policy.

10. Accountability and Record-Keeping

Who is responsible for data protection?

All of our volunteers are responsible for data protection and each person has his/her role to play to make sure that we are compliant with Data Protection laws.

The Data Protection Officer shall support the Board and members of the organisation in their responsibility for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other data protection-related policies, and with the GDPR and other applicable data protection legislation.

Rugby League Ireland maintains Records of Processing Activities (RoPA) in accordance with Article 30 of the GDPR. These records document the categories of personal data processed, purposes of processing, lawful bases, retention periods, and security measures.

Records of Processing Activities are reviewed periodically and updated where necessary to reflect changes in processing activities.

The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

- The name and details of the Company and any applicable third-party data processors
- The purposes for which the Company collects, holds, and processes personal data
- Details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates

Rugby League Ireland maintains Records of Processing Activities (RoPA) in accordance with Article 30 of the GDPR. These records document the categories of personal data processed, purposes of processing, lawful bases, retention periods, and security measures.

Records of Processing Activities are reviewed periodically and updated where necessary to reflect changes in processing activities.

- Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards
- Details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Policy) and
- Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

Rugby League Ireland may engage third-party service providers to process personal data on its behalf in support of its administrative, operational, and regulatory functions. Where third-party data processors are engaged, Rugby League Ireland ensures that such processors provide sufficient guarantees to implement appropriate technical and organisational measures so that processing meets the requirements of the General Data Protection Regulation.

All third-party data processors engaged by Rugby League Ireland are subject to written data processing agreements that comply with Article 28 of the GDPR and set out the processor's obligations, including confidentiality, security, sub-processing restrictions, and assistance with data subject rights and data breach management.

Rugby League Ireland takes reasonable steps to ensure that personal data processed by third-party processors is used only for authorised purposes and is protected against unauthorised or unlawful processing, accidental loss, destruction, or damage.

11. Data Protection Impact Assessments

The Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR.

Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

- The type(s) of personal data that will be collected, held, and processed
- The purpose(s) for which personal data is to be used
- The Company's objectives
- How personal data is to be used
- The parties (internal and/or external) who are to be consulted
- The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed
- Risks posed to data subjects
- Risks posed both within and to the Company and
- Proposed measures to minimise and handle identified risks.

12. Keeping Data Subjects Informed

The Company shall provide the information set out below to every data subject. It will do this primarily through the issue of its Privacy Notice:

Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection and

Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

a) if the personal data is used to communicate with the data subject, when the first communication is made or
b) if the personal data is to be transferred to another party, before that transfer is made or
c) as soon as reasonably possible and in any event not more than 30 days after the personal data is obtained

The following information shall be provided:

Details of the Company including, but not limited to, the identity of all of its employees are responsible for data protection and each person has his/her role to play to make sure that we are compliant with Data Protection laws.

- The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing
- Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data
- Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed.

Where the personal data is to be transferred to one or more third parties, details of those parties:

- Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 28 of this Policy for further details)
- Details of data retention
- Details of the data subject's rights under the GDPR
- Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time
- Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR)
- Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it and
- Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

13. Data Subject Access

Data subjects may make Subject Access Requests ("**SARs**") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data and why.

Data subjects wishing to make a SAR may do so in writing, using the Company's Subject Access Request Form, or other written communication. SARs should be addressed to the Company's Data Protection Officer.

Responses to SARs shall normally be made within 30 days of receipt, however, this may be extended by up to 60 days if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

All SARs received shall be handled by the Data Protection Officer.

The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a

data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. Rectification of Personal Data

Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

The Company shall rectify the personal data in question, and inform the data subject of that rectification, within 30 days of the data subject informing the Company of the issue. The period can be extended by up to 60 days in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

15. Erasure of Personal Data

Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

- It is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed
- The data subject wishes to withdraw their consent to the Company holding and processing their personal data
- The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 18 of this Policy for further details concerning the right to object)
- The personal data has been processed unlawfully
- The personal data needs to be erased in order for the Company to comply with a particular legal obligation.

Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within 30 days of receipt of the data subject's request. The period can be extended by up to 60 days in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. Restriction of Personal Data Processing

Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. Data Portability

The Company does not process personal data using automated means.

Where data subjects have given their consent to the Company to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the Company and the data subject, data subjects have the right, under the GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers)

To facilitate the right of data portability, the Company shall make available all applicable personal data to data subjects in the following format[s]:

- Hard copy – registered post
- Email with PDF documents

Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

All requests for copies of personal data shall be complied with 30 days of the data subject's request. The period can be extended by up to 60 days in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

18. Objections to Personal Data Processing

Data subjects have the right to object to the Company processing their personal data based on legitimate interests, direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims

Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately

Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the GDPR, "demonstrate grounds relating to his or her particular situation". The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

19. Automated Decision-Making

The Company currently does not use personal data in automated decision-making.

20. Profiling

The Company currently does not use personal data for profiling purposes.

21. Personal Data Collected, Held and Processed

All personal data is collected, held, and processed by the Company is recorded in a Register of Data Processing Activities.

22. Data Security - Transferring Personal Data

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

- Personal data may be transmitted over secure networks only
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable
- Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
- Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using An Post or approved courier services and
- All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked “confidential”.

23. Data Security - Storage

The Company shall ensure that the following measures are taken with respect to the storage of personal data:

- All electronic copies of personal data should be stored securely using passwords data encryption
- All hard copies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
- All personal data stored electronically should be backed up in accordance with the Company’s backup policy
- No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Company or otherwise without the approval of management and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary; and
- No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken)

24. Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Company’s Data Retention Policy.

25. Data Security - Use of Personal Data

The Company shall ensure that the following measures are taken with respect to the use of personal data:

- Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time
- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it and
- Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Marketing function to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service.

26. Data Security - IT Security

The Company shall ensure that the appropriate and industry recognised good practises are taken with respect to IT and information security.

27. Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

All employees, volunteers, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy

Only employees, volunteers, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company

All employees, volunteers, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so

All employees, volunteers, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised

All employees, volunteers, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise

Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed

All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy

The performance of those employees, volunteers, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed

All employees, volunteers, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract

All agents, volunteers, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the GDPR and

28. Transferring Personal Data to a Country Outside the EEA

The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

- The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data
- The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority
- The transfer is made with the informed consent of the relevant data subject(s)

The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject)

- The transfer is necessary for important public interest reasons
- The transfer is necessary for the conduct of legal claims
- The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent or
- The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

29. Data Breach Notification

All personal data breaches must be reported immediately to the Company's Data Protection Officer.

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Company's Data Protection Officer must ensure that the Data Protection Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 29.2) to the rights and freedoms of data subjects, the Company's Data

Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay

Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the Company's Data Protection Officer (or another contact point where more information can be obtained)
- The likely consequences of the breach
- Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Any breaches of this Policy will be viewed very seriously. All employees must read this Policy carefully and make sure that they are familiar with it. Breaching this Policy is a disciplinary offence and will be dealt with under our Disciplinary Procedure.

If you do not comply with data protection laws and/or this Policy, then you are encouraged to report this fact immediately to the Company's 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 the Company's Data Protection Officer. Our Whistleblowing Procedure will apply in these circumstances and you may choose to report any non-compliance or breach through our confidential whistleblowing reporting facility.

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/contractor, failure to comply with our policies could lead to termination of your volunteering/contractor 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.

<u>For the Organisation</u>:

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

Civil Fines: These can be up to Euro €20 million.

Assessments, investigations and enforcement action: We could be assessed or investigated by, and obliged to provide information to the Data Protection Commissioner's Office on its processes and procedures and/or subject to the Data Protection Commissioner's Office'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.

30. Implementation of Policy

This Policy shall be deemed effective as of X January 2026. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: Jim Reynolds

Position: Chairman, Rugby League Ireland

Date: X January 2026

Due for Review by: This policy was last reviewed and updated in **2025** and will be reviewed on a periodic basis, or earlier where required due to changes in legislation, guidance, or organisational practices.

Signature: