2023

Data Protection and Privacy Policies

Eventing IRELAND

Grass Roots to Gold Medals

Eventing Ireland

11/27/2023

Content

Data Protection Policy

1 Data Protection Policy

1.1 Introduction

In its everyday business operations Eventing Ireland ("we", "us, "our") makes use of a variety of personal data which identifies individuals. The use of such information is governed by specific legislation and we, as a Data Controller, must comply with certain obligations laid down in law.

The purpose of this policy is to outline how we comply with current data protection legislation which includes the Data Protection Act, 2018 ("the Act") and the General Data Protection Regulation 2016/679 ("GDPR").

The policy covers both personal and special categories of personal data processed by us. The policy applies equally to personal data held in both manual and electronic forms. All personal data and special categories of personal data will be treated with equal care by us. Both categories will be equally referred to as personal data in this policy, unless specifically stated otherwise.

This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to Eventing Ireland systems.

1.2 Definitions

There are a total of 26 definitions listed within the GDPR and it is not appropriate to reproduce them all here. However, the most fundamental definitions with respect to this policy are as follows:

Personal data is defined as:

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;

'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;

2 Types of Personal Data

At Eventing Ireland, we collect, process and store certain types of personal data in order to carry out our services. Such data includes:

General: name, address, date of birth, email, telephone numbers, photo

Financial data: card details are not stored where the card numbers are visible

Membership data: identification documents, club details, grading details, horse details, achievements

Special Category data: health data (only in certain circumstances)

Data collected through other channels: Photos and videos at events, email correspondence through interaction with us

Other data: Cookies on our website, IP addresses

3 Data Protection Fundamentals

3.1 Principles Relating to Processing of Personal Data

There are a number of fundamental principles upon which the GDPR is based. These are as follows:

1. Personal data shall be:

   (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency**');

   In practice this means that we will ensure that we identify a lawful basis for all processing, we never use personal data in a way that individuals would not expect and we clearly communicate how we use people's data.

   (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');

   In practice this means that we only use data for the reason that we collected it.

   (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

   In practice this means we only collect the minimum amount of personal data needed.

   (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

   In practice this means that we are careful to ensure all data is accurate and that we correct any inaccuracies without delay.

   (e) 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; ('storage limitation');

In practice this means that we recognise that we cannot keep all data forever and so we implement retention periods accordingly.

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

In practice this means that we ensure we have adequate measures in place to protect the data we store, these measures are documented in our Technical and Organisational Measures.

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('**accountability**').

Eventing Ireland will ensure that it complies with all of these principles and that we are able to demonstrate our compliance.

3.2 Rights of the Individual

The data subject also has rights under the GDPR. It is important to note that these are not absolute rights and restrictions, exemptions or limitations may apply. These consist of:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Each of these rights are supported by appropriate procedures within Eventing Ireland that allow the required action to be taken within the timescales stated in the GDPR. We will ensure that we will respond to all requests in a timely manner and valid data access requests will be responded to within 1 month of the date the request was received.

3.3 Lawfulness of Processing

We are obligated to define a lawful basis for processing personal data. Below is a summary of our use of personal data and the lawful basis we rely on for the processing of different categories of data for different purposes.

Lawful Basis	Purpose/s	Data Categories
Consent	If we collect medical information from individuals, we will request their explicit consent. This information is not stored. To keep members up to date on news and events through our newsletter, all communications include an opt-out. Visitors to our website are asked to consent/or not to cookies.	Medical information Email Cookie preference, device details
Performance of a Contract	A contractual relationship exists where individuals become a member. We must collect specific information to facilitate membership.	Name, address, date of birth, gender, email, phone number/s, region, grades, photo, parent/guardian details

Lawful Basis	Purpose/s	Data Categories
		(if relevant)
Legal Obligation	We are legally obliged to collect certain information to meet our obligations as an employer	Details collected from staff will be outlined in the Employee Privacy Notice (See 6). Data categories will include all those required by law.
Vital Interests of the Data Subject	There may be instances if an individual is involved in an accident, that we will disclose their details to protect their vital interests	Contact details, membership information, next of kin
Task Carried Out in the Public Interest	Generally, we do not rely on this lawful basis. This may apply if we receive instructions from public health authorities regarding the processing of certain information.	At present we do not carry out any processing in the Public Interest
Legitimate Interests	Where members look to participate in an event, certain data must be processed for this purpose. This is in the interests of both parties. If members wish to participate in a draw or competition, we will collect certain contact information. Through the general administration of memberships, we must process certain personal data in order to provide our services to members. We issue communications to members containing news and information we deem to be of interest to them. They can opt-out of receiving such communications at any time.	Contact details, membership information, grades

3.4 Privacy by Design

Eventing Ireland has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect, or process personal data will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments.

The data protection impact assessment will include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the personal data
- What controls are necessary to address the identified risks and demonstrate compliance with legislation

Use of techniques such as data minimisation and pseudonymisation will be considered where applicable and appropriate.

4 Data Sharing and Transfers

We do not sell any personal information, nor do we share it with unaffiliated third parties unless we are required to do so by law. We will ensure that any information passed to third

parties conducting operational functions on our behalf will be done with respect for the security of personal data and will be protected in line with data protection law.

Ways in which we may share personal information include:

- With official bodies including, but limited to:
  - the Revenue Commissioners in relation to legal submissions as an Employer
  - the Gardai, we reserve the right to report to law enforcement any activities that we, in good faith, believe to be illegal;
- With event organisers around Ireland where the data is required to facilitate an individual's participation in an event.
- With clubs as part of their affiliation with Eventing Ireland.
- To engage external IT providers so as to ensure the security of our IT systems in order to protect all personal data.
- With our insurers or assessors when providing or reviewing information in the event of an incident occurring.
- To engage professional services of third parties, such as auditors, solicitors or any other such business advisers. Any such parties are bound by confidentiality.

Eventing Ireland will ensure that all relationships it enters into that involve the processing of personal data are subject to a documented contract that includes the specific information and terms required by the GDPR.

4.1 International Transfers of Personal Data

At present, the only personal information that we transfer outside the EEA is an email address and this is done through the use of MailChimp in order to circulate our newsletter. We have received a copy of MailChimps data-processing-addendum which governs the sharing of data between Eventing Ireland in the EU and MailChimp in the US. Additionally, MailChimp, as part of the Intuit Group have signed up the (EU-US Data Privicy Framework). This means that the data sharing is covered under the Adequacy Agreement between the European Commission and the US.

5 Data Protection Officer

Having reviewed the requirements of Article 37 GDPR, we have determined that Eventing Ireland does not currently require a Data Protection Officer to be appointed.

6 Breach Notification

Article 4(12) GDPR defines a 'personal data breach' as:

"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"

Our staff are trained to recognise a breach and are instructed to inform the General Manager immediately if they suspect a breach has occurred or have evidence of a potential breach.

It is Eventing Ireland's policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with Article 33 GDPR, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed within 72 hours. Where there is deemed to be a high risk to the rights and freedoms of individuals, all reasonable effort will be taken to inform the individuals themselves.

Each incident will be assessed and managed on a case-by-case basis.

7 Data Access Requests

An individual has the right to be informed whether we hold data/information about them and to be given a description of the data together with details of the purposes for which their data is being kept. The individual must make this request to us in writing, and we will accede to the request within one month having first verified the identity of the requester to ensure the request is legitimate.

Where a subsequent or similar request is made soon after a request has just been dealt with, it is at the discretion of EI whether or not it needs to comply with the second request. This will be determined on a case-by-case basis. In cases where we process a large quantity of information concerning the data subject, we may request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

No personal data can be supplied relating to another individual unless that third party has consented to the disclosure of their data to the applicant. Data will be carefully redacted to omit references to any other individual and only where it has not been possible to redact the data to ensure that the third party is not identifiable, we must refuse to furnish the data to the applicant.

Individuals are asked to be clear and concise when making a Data Access Request, though it is not mandatory to be specific about the data being sought. Once we have verified the identity of the requester and the request is not deemed to be manifestly unfounded or excessive, we will comply with the request at no charge to the data subject and within one month. At times it may be necessary to extend the response period by applying a 2-month extension. Where we deem this to be justified, individuals will be informed of the reasoning for the extension.

The General Manger will manage and respond to Data Access Requests.

8 Security of Personal Data

We ensure the confidentiality, integrity, availability, and resilience of personal data when in use, transit and storage. We are obliged to protect the data from inadvertent destruction, amendment, loss, disclosure, corruption or unlawful processing.

- Appropriate security controls, including technical and non-technical are utilised to protect personal data
- All confidential personal data is only accessible to authorised personnel
- Personal data held in manual (paper) files is held securely in locked cabinets
- Data printouts are shredded and disposed of securely when no longer required
- Staff are instructed to always keep information strictly confidential and not to disclose or discuss any confidential personal information with any unauthorised outside parties
- Our IT partners ensure that our systems are protected and that backups are done and stored securely
- Staff and volunteers are given regular training on how best to protect the personal data they handle during the course of their work
- Any third parties who process personal data on our behalf are contractually bound to process personal data in line with current data protection law practices and principles thus ensuring the security of the data

9 Data Retention

We will only retain personal data for as long as necessary to fulfil the purpose(s) for which it was obtained, considering any legal/contractual obligation to keep it. Where possible we record how long we will keep all data, where that is not possible, we will explain the criteria for

the retention period. Once the retention period has expired, the respective data will be permanently deleted.

10 Review

This policy will be reviewed at least annually or in line with any changes in processing.

Document Ref.	EI-GDPR POL V.3
Version:	**3**
Dated:	**November 2023**
Revision Due:	**November 2024**

Eventing Ireland Privacy Policies

1 Online Services Privacy Notice

This Privacy Notice provides information about the ways in which Eventing Ireland collects, processes and stores the personal data provided through the use of our online services. This Notice is meant as a summary only, our long form Data Protection Policy is available upon request with further information on our processing.

Our registered address is Beech House, Millennium Park, Osberstown, Naas, Co. Kildare, Ireland. You can contact us by email at alison@eventingireland.com or by telephone on +353 (0)83 020 0414. Our Company Registration Number is 2486.

1.1 Personal data we collect

We collect certain personal data when you:

- register to use our services
- sign up for membership
- upload documentation electronically
- avail of our services provided
- contact us via our website

We will collect some or all of the following information depending on your use of our online platforms:

- name, address, date of birth, email, telephone numbers, club details, grading information, health information (where applicable), ID verification documentation, photo, device details, location data.

1.2 Principles of Processing Personal Data

All data processed by us is done so in line with the principles of data processing, these are:

- **lawfulness, fairness and transparency** – we will always process data lawfully and we will be clear, open and honest about how the data is used.
- **purpose limitation** – we will only use personal data in line with the services on our website, data will not be used for further purposes.
- **data minimisation** – we will only collect the minimum amount of data required to carry out our services.
- **accuracy** – we will ensure that we record data accurately.
- **storage limitation** – we apply retention periods to the data received.
- **integrity and confidentiality** – we have appropriate technical and organisational measures in place to protect all data collected, processed and stored by us.
- **accountability** – as a Data Controller we are responsible for and will be able to demonstrate compliance with the above principles.

1.3 What is our legal basis for using your personal data?

We must have a legal basis for using your personal data, these are as follows:

- Performance of a contract – during membership application process and when you become a member, we must collect certain data to provide our services.
- Legitimate interests – we sometimes collect and use your personal data because we have a legitimate reason to use it, and this is reasonable when balanced against your right to privacy. eg. when inquiring about or registering for events.
- Consent – we rely on your consent for certain processes such as when you indicate that you consent to receive marketing information.

1.4 How do we use your personal data?

We will use your personal data for some or all of the following, depending on your use of our online services:

- To process your membership details
- Administering your membership and the services we provide to you,
- Verifying your identity and the information you provide to us,
- Facilitating the provision of additional services, such as competition entry,
- Assessing how we can improve the products and services we provide to you with and future services which may be of interest,
- For providing updates about our services by way of our news letter unless you have opted out of receiving such communications,
- Obtaining information about your general use of our website.

1.5 How do we protect your personal data?

We use a variety of physical and technical measures to keep your personal data safe and prevent any unauthorised access or disclosure. Electronic data and databases are stored on secure computer systems with control over access to information using both physical and electronic means. Our staff receive data protection and information security training. We have policies in place which staff are required to follow when they handle your personal data.

1.6 How long will we keep your personal data?

We will generally keep your personal data for seven years after our relationship with you ends or such period as may be required by applicable laws. We may keep your personal data for longer because of a potential or ongoing investigation or another legal reason.

1.7 Do we share your personal data with anyone?

Data Sharing

We may share your personal data as required with affiliated bodies.
We may also share your information with third party agents or subcontractors who work on our behalf and provide us with expertise or assistance in such areas as legal, accounting, IT or insurance. We have contracts in place with these agents or subcontracts to ensure the protection and security of your personal data.

Where we outsource the processing of personal data, we do so under a Data Processing Agreement.

Data Transfers

At present, the only personal information that we transfer outside the EEA is an email address and this is done through the use of MailChimp in order to circulate our newsletter. We have received a copy of MailChimps data-processing-addendum which governs the sharing of data between Eventing Ireland in the EU and MailChimp in the US. Additionally, MailChimp, as part of the Intuit Group have signed up the (EU-US Data Privicy Framework). This means that the data sharing is covered under the Adequacy Agreement between the European Commission and the US. Please also refer to 4.1

1.8 Your privacy rights

You have a number of rights regarding the processing of your personal data, these are:

- You have the right to be told about how we use your personal data and for copies of any data we hold in relation to you.
- You can ask us to correct your personal data if you think it's wrong.
- You can ask us to delete your personal data.
- You can object to us processing your personal data for marketing purposes.

- You can object to us processing other personal data (if we are using it for legitimate interests)
- You can ask us to restrict how we use your personal data.
- You can ask us to transfer personal data to you.
- You can ask us to carry out a human review of an automated decision we make about you. Please note: we do not use any automated decision making at present so this right is not applicable.

Please note that the above rights are not absolute, and some restrictions and limitations may apply.

You also have the right to lodge a complaint with the relevant supervisory authority, which in Ireland is, the Data Protection Commission, info@dataprotection.ie.

1.9 Cookies

What Are Cookies

Cookies are small files that store information on your hard drive or browser that means that the website can recognise that you have visited the website before. They make it easier for you to maintain your preferences on the website, and by seeing how you use the website we can tailor the website around your preferences and measure usability of the website.

What Do We Use Cookies For

We may collect information about your computer, including where available your IP address, operating system and browser type, for system administration, to help us provide a better service; to record session information and/or to assist you in browsing the website. This may in some instances only be statistical data about how you browse our website. Cookies cannot be used to run programs or deliver viruses to your computer. Cookies are uniquely assigned to you and can only be read by a web server in the domain that issued the Cookie to you. For the same reason, we may obtain information about your usage of the website by using a cookie file which is stored on the hard drive of your computer. Cookies contain information that is transferred to your computer's hard drive. Cookies help us to improve the website and to deliver a better and more personalised service. They enable us:

- to estimate usage numbers and patterns;
- to store information about your preferences, and so allow us to customise the website according to your individual interests;
- to speed up your searches; and
- to recognise you when you return to the website.

We do not currently use any analytics on our website.

Managing Cookies Usage

You may refuse to accept, or you may disable cookies by activating the setting on your browser which allows you to refuse the setting of cookies. However, if you select this setting, you may be unable to access certain parts of the website or unable to avail of our services. Unless you have adjusted your browser setting so that it will refuse cookies, our system will issue cookies when you log on to the website.

You can find out how to do this for your particular browser by clicking "help" on your browser's menu or by visiting www.allaboutcookies.org.

If you have any concerns about material which appears on the website, please contact us.

1.10 External Links

Any external links to other websites are clearly identifiable as such and Eventing Ireland (EI) is not responsible for the content or the privacy statements of these websites. If you have any issues or queries relating to such websites, please contact the providers directly.

Updates to our privacy notice and contact

We may update our Privacy Notice from time to time. If we modify our Privacy Notice, we will publish the revised version on our website.

If you have any questions, concerns or suggestions related to our Privacy Notice, you can contact us by emailing alison@eventingireland.com.

2 Volunteer Privacy Notice and Guidelines

Eventing Ireland collects and processes personal data relating to our volunteers. We are committed to being transparent about how we collect and use that data and to meeting our data protection obligations under the Data Protection Act 2018 (the Act) and the General Data Protection Regulation 2016/679 (GDPR).

Please note that there may be elements of the notice that are not applicable to you according to the specific role you undertake.

2.1 What information do we collect?

We collect and process a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number
- the details of your role as a volunteer
- details of participation training courses
- details of participation in meetings
- images and videos of you during participation in activities and events;

2.2 How do we collect your personal data?

We collect this information in a variety of ways. For example, data is collected through:

- through references you have provided
- correspondence with you
- through meetings or other interaction with you such as email correspondence
- generally, through the course of your work as a volunteer
- through photos and videos taken during events and activities

2.3 Why do we process personal data?

In most cases, we have a legitimate interest in processing personal data before, during and after the end of the relationship. We rely on the lawful basis of legitimate interests for processing involving:

- to ensure the security and compliant use of our IT systems – we are obliged to have appropriate technical and operations securities in place
- to promote Eventing Ireland through promotional campaigns on our website and social media platforms – it is important ensure continued growth and guarantee the sustainability and growth of the organisation.

Processing volunteer data allows us to:

- run a recruitment process for volunteers
- maintain accurate and up-to-date volunteer records and contact details
- to carry out regular volunteer training
- respond to and defend against legal claims
- to gather evidence for possible grievance processes
- to promote Eventing Ireland through our website and social media platforms by celebrating achievements.

In limited circumstances special categories of data will be processed only with your explicit consent. We may also need to process this data for the establishment, exercise or defence of legal claims.

2.4 Who has access to data?

Your information will be shared internally with the management team and Directors, when necessary, in the performance of their duties and is kept strictly confidential at all times.
Ways in which we may share personal information include:

- to engage external IT providers so as to ensure the security of our IT systems in order to protect all personal data.

- with our insurers or assessors when providing or reviewing information in the event of an incident occurring.
- to engage professional services of third parties, such as solicitors or any other such business advisers. Any such parties are bound by confidentiality.
- we reserve the right to report to law enforcement any activities that we, in good faith, believe to be illegal.

Eventing Ireland will not transfer your data to countries outside the European Economic Area.

2.5 How do we protect your data?

We have internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by those parties listed in this policy in the performance of their duties.

Where we engage third parties to process personal data on our behalf, they do so on the basis of written instructions in a Data Processing Agreement, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of your data.

2.6 Your rights

Under data protection law, you have a number of rights, these include:

- the right to have personal information processed in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- the right to be informed, this means that we need to tell you what data we are using, why we are using it and for what purpose as well as informing you of the details of any third parties in receipt of data from us.
- the right of access, you are allowed to see what data of yours we are processing if you request that from us.
- the right of rectification, that means if the data we are using is incorrect we must correct it.
- the right to erasure (or right to be forgotten), this means that you have the right to issue a request to us requesting the erasure of your personal data. However, in certain cases, we will have overriding legitimate grounds for continued processing, and we may be unable to comply with such a request.
- the right to restrict processing, this means that you can ask you to stop using your data unless we have a legitimate lawful purpose for continuing to do so.
- the right to data portability, this means that you have the right to move your data to another controller and we must provide you with a copy of your data “in a structured, commonly used and machine-readable format”.
- the right to object, this means that you can object to the use of your data and we must stop using it unless we have an overriding legitimate reason to continue.
- the right not to be subject to automated decision making, including profiling.

Please be aware that these are not absolute rights and restrictions, exemptions and limitations may apply. If you would like to exercise any of these rights, please contact the General Manager by emailing alison@eventingireland.com.

If you believe we have not complied with your data protection rights, you can complain to the Data Protection Commission by contacting them through their website www.dataprotection.ie.

2.7 Your Data Protection Responsibilities

In every instance when you are working with another individual’s personal data you must make sure to think at all times about the security of that data, this could be data belonging to Eventing Ireland staff or data relating to a member, volunteer or any other third party. It is advisable for volunteers to read our Data Protection Policy so as to ensure that you follow certain guidelines relating to the security of personal data.

These guidelines include:

- make sure that any devices used to access Eventing Ireland data have appropriate securities such as up to date anti-virus software, passwords
- never store records containing personal information in an unsecure location
- always keep information strictly confidential and do not disclose or discuss personal data or circumstances with any unauthorised outside parties.

2.8 Personal Data Breaches

Article 4(12) GDPR defines a 'personal data breach' as:
"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".

In the event of a breach of personal data occurring, it is vital to ensure that it is dealt with immediately and appropriately to minimise the impact of the breach and prevent a recurrence. If you become aware of an actual, potential, or suspected breach of personal data, you must report the incident to the General Manager immediately.

You are never permitted to take action yourself in the event of a breach, even if you have caused the breach, only specific staff are authorised to do so.

2.9 Conclusion

At Eventing Ireland, we take the privacy of our volunteers seriously and we respect your rights and freedoms. Should you be concerned about your rights, you should contact the General Manager by emailing alison@eventingireland.com.

We reserve the right to update or amend this Notice at any time deemed appropriate to reflect any changes in our processing.

3 Technical & Organisational Measures

Introduction

This TOMs document describes the security measures we have in place to protect the data that we process in order that we can meet our obligations to keep all data secure. This document should be read alongside our Data Protection Policy.

Security Measures

3.1 Staff Awareness

All staff are made aware of the importance of data security and are informed that should never click on a link in an email or open an attachment if they are unsure about the source of the email. Staff are also given guidelines with regard to conduct on social media and their own responsibility to protect the personal data they access during the course of their work.

Staff are aware of their obligation to report any actual or potential data breaches immediately upon becoming aware.

3.2 Confidentiality

All staff and volunteers are bound by a duty of confidentiality and are obliged to sign a confidentiality agreement upon commencement of their position.

3.3 Access

We have implemented the following measures for access to systems where personal data is stored:

- For every employee, a personally assigned user is set up with a password.
- Passwords must be unique and may not be used for other accounts. Passwords must be changed annually and never shared or disclosed.
- Only employees get access to the majority of data, volunteers (ie: event organisers) are only given access to data directly relevant to their role.

3.4 Devices

Employees are equipped with devices owned by Eventing Ireland. Anti-virus software is installed and updated regularly, and staff are instructed that these devices should not be accessed by any other individuals for any purpose.

Staff are informed that they are not permitted to download applications or software to these devices unless instructed by Eventing Ireland and in consultation with our IT providers.

3.5 Technical Security

We ensure that we have regularly updates and security patches to protect our systems. Computer viruses and malware are the most common method used to exploit vulnerabilities. In addition to security patching, we shall ensure that suitable anti-virus software is installed on all information systems including servers, laptops, computers and mobile devices.

3.6 Physical Security

Staff are aware of the importance of ensuring that all records are physically secure. Paper documentation containing personal data must never be stored where it is accessible to third parties. All devices must be locked when not in use and stored securely at all times.

3.7 IT Service Providers

We have engaged Esker Software Ltd. and Vitamin Creative Ltd. for their expertise in the area of data management and security. We have a Master Services Framework Agreement with these companies.

3.8 Data Sharing

We will ensure that if we engage a third party to process data on our behalf, that we will do so under a Data Processing Agreement and data will only be shared with parties who can demonstrate their compliance to data protection legislation.

3.9 Data Storage

We use Microsoft 365 Office packages, and all data is stored within the EU. Our member database is stored on Amazon Web Servers in Ireland with backups in the EU.

3.10 Disposal of Information Systems

Information systems due for disposal may still hold important data. Such systems include servers, laptops, computers and mobile devices, amongst others. When disposing of outdated information systems, we shall ensure that data residing on these systems is destroyed.

We will always dispose of devices using service providers that offer a certificate of destruction.

Review

Eventing Ireland will continue to review its compliance measures and any updates to our TOMs will be detailed in this document which will be reviewed at least annually.

4 WhatsApp Usage Guidelines

At the outset individuals must consent prior to being put into a WhatsApp Group as their telephone number will be visible to all within the group, and personal telephone numbers should not be communicated without consent.

1. You must retain a record so as to demonstrate that consent was obtained from each individual prior to them being added to a group.

2. The first message must clearly communicate what the WhatsApp Group is for and who is responsible for the administration.

3. If all members can post and not just the administrators, you should state what is expected with regard to conduct and content when members are posting.

4. The group is intended as a convenient way to distribute information to Group members quickly and efficiently regarding Eventing Ireland matters only, it is not intended as a platform for personal messages.

5. The following ought to be adhered to:

    a. The group is not to be used to discuss non-Eventing Ireland related issues.
    b. The group should not be used to express personal opinions or post private messages.
    c. Any opinions expressed are the opinions of individual members.
    d. Administrators should delete any irrelevant messages.
    e. Administrators should delete any inappropriate messages. Content deemed inappropriate would be:

        i. using inappropriate language,
        ii. insulting messages,
        iii. voicing grievances with Eventing Ireland or any other individuals,
        iv. comments regarding any individuals that may be deemed defamatory, derogatory, offensive, accusatory, confrontational or negative in any way.

6. Group members who post inappropriate messages should be warned initially and if the behaviour continues, they should be removed from the Group.

7. Inform members when a reply is required, otherwise members should be advised not to respond to every message as continuous notification can be annoying for members and undermine the efficiency of the facility.

8. In the event that there is a breach of any of the rules, the group administrator reserves the right to remove the transgressor from the group.

9. Participation in WhatsApp Groups is not obligatory, Group members may choose to leave at any time without detriment.

10. Respect everyone's privacy – being part of a WhatsApp group requires mutual trust.

Thank you for abiding by these guidelines.

5 Social Media Guidelines - Staff

Social media is the collective term referring to social and professional networking sites (for example Facebook, LinkedIn, Twitter, Instagram), blogs, boards and other similar online platforms and these guidelines extend to all such sites and incorporates any future developments of such media. Breaches of Eventing Ireland's social media guidelines will be investigated, and we retain the right to take disciplinary action, up to and including dismissal.

5.1 Applies to all Staff

At Eventing Ireland, we recognise that staff use social media platforms as part of their daily lives. Staff should always be mindful of what they are posting, who can see it, and how it can be linked back to the organisation and work colleagues.

All staff should be aware that the organisation regularly monitors the internet and social media in reference to its work and to keep abreast of general internet commentary, brand presence and public perceptions. The organisation does not specifically monitor social media sites for employee content on an ongoing basis, however staff should not expect privacy in this regard. The organisation reserves the right to utilise for disciplinary purposes any information that could have a negative effect on the organisation or its staff, which management comes across in regular internet monitoring, or is brought to the organisation's attention by staff, volunteers, members, or any other individuals.

All staff are prohibited from using or publishing information on any social media sites, where such use has the potential to negatively affect the organisation or its staff. Examples of such behaviour include, but are not limited to:

- publishing material that is defamatory, abusive or offensive in relation to any employee, manager, volunteer, member or any other individual affiliated with the organisation;
- publishing any confidential or business-sensitive information about the organisation; and
- publishing material that might reasonably be expected to have the effect of damaging the reputation or professional standing of the organisation.

5.2 Rules Regarding Usage

All staff must adhere to the following when engaging in social media.

1. Be aware of your association with the organisation when using online social networks. You must always identify yourself and your role if you mention or comment on the organisation. Where you identify yourself as an employee, ensure your profile and related content is consistent with how you would present yourself with colleagues and members. You must write in the first person and state clearly that the views expressed are your own and not those of the organisation. Wherever practical, you must use a disclaimer saying that while you work for the organisation, anything you publish is your personal opinion, and not necessarily the opinions of the organisation.
2. You are personally responsible for what you post or publish on social media sites. Where it is found that any information breaches any organisation policy, such as breaching confidentiality or bringing the organisation into disrepute, you may face disciplinary action up to and including dismissal.
3. Be aware of data protection rules – you must not post colleagues' details or pictures without their individual consent. Photographs of company events should not be posted online without the prior express consent of the General Manager.
4. Material in which the organisation has a proprietary interest must not be transmitted, sold, or otherwise divulged, unless the organisation has already released the

information into the public domain. Any departure from these guidelines requires the prior written authorisation of your manager.

5. Be respectful at all times, in both the content and tone of what you say. Show respect to your audience, your colleagues and organisation members and suppliers. Do not post or publish any comments or content relating to the organisation or its staff, which would be seen as unacceptable in the workplace or in conflict with the organisation's ethos. Make sure it is clear that the views and opinions you express are your own.
6. Recommendations, references, or comments relating to professional attributes, are not permitted to be made about staff, former staff, volunteers, members or any individuals affiliated with the organisation on social media and networking sites. Such recommendations can give the impression that the recommendation is a reference on behalf of the organisation, even when a disclaimer is placed on such a comment.
7. Once in the public domain, content cannot be retracted. Therefore, always take time to review your content in an objective manner before uploading. If in doubt, ask someone to review it for you. Think through the consequences of what you say and what could happen if one of your colleagues had to defend your comments to a member.
8. If you make a mistake, be the first to point it out and correct it quickly. You may factually point out misrepresentations, but do not create an argument.
9. It is very important that staff immediately report any inappropriate activity or behaviour regarding the organisation, its staff or third parties. All allegations made in good faith will be fully and confidentially investigated. You are required to cooperate with all investigations of alleged violations.
10. These guidelines extend to future developments in internet capability and social media usage.

In addition to the above rules, there are a number of key guiding principles that staff should note when using social media tools:

- always remember on-line content is never completely private;
- regularly review your privacy settings on social media platforms to ensure they provide you with sufficient personal protection and limit access by others;
- consider all online information with caution as there is no quality control process on the internet and a considerable amount of information may be inaccurate or misleading;
- at all times respect copyright and intellectual property rights of information you encounter on the internet. This may require obtaining appropriate permission to make use of information. You must always give proper credit to the source of the information used.

5.3 Enforcement

Non-compliance with the general principles and conditions of these social media guidelines and any related internet, e-mail and confidentiality policies may lead to disciplinary action, up to and including dismissal.

These guidelines are not exhaustive. In situations that are not expressly governed by these guidelines, you must ensure that your use of social media and the internet is at all times appropriate and consistent with your responsibilities towards the organisation. In case of any doubt, you should consult with your manager.

Monitoring of internet usage applies to personal use as well as normal business use.

6 Employee Privacy Notice and Operational Guidelines

6.1 Introduction

Eventing Ireland collects and processes personal data relating to our employees to manage the employment relationship. We are committed to being transparent about how we collect and use that data and to meeting our data protection obligations under the Data Protection Act 2018 (the Act) and the General Data Protection Regulation 2016/679 (GDPR).

6.2 Personal Data

Examples of the personal data we process about you as a member of our staff includes:

- your name, address and contact details, including email address and telephone number, date of birth and gender.
- the terms and conditions of your employment.
- details of your qualifications, skills, experience and employment history, including start and end dates.
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover.
- details of your bank account and PPSN.
- information about your marital status, next of kin, dependants and emergency contacts
- information about your nationality and entitlement to work in Ireland.
- details of your schedule (days of work and working hours) and attendance at work.
- details of periods of leave taken by you, including holiday, sickness absence, family leave and the reasons for the leave.
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence.
- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence.
- information about medical or health conditions, including whether or not you have a disability for which we need to make reasonable adjustments.
- details of trade union membership if relevant.
- images and videos of you during participation in Eventing Ireland activities and events.

6.3 Collection of Personal Data

We collect this information in a variety of ways. For example, data is collected through:

- application forms.
- CVs.
- correspondence with you.
- through interviews, meetings or other assessments.
- generally through the course of your work.
- through photos and videos taken during events and activities.

6.4 Purposes for Processing Personal Data

We need to process data to enter into an employment contract with you and to meet our obligations under your employment contract. For example, we need to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer any relevant benefits.
In some cases, we need to process data to ensure that we are is complying with our legal obligations. For example, we are required to check an employee's entitlement to work in Ireland and to deduct tax.

In other cases, we have a legitimate interest in processing personal data before, during and after the end of the employment relationship.

Processing employee data allows us to:

- carry out a recruitment process.
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights.
- operate and keep a record of disciplinary and grievance processes.
- operate and keep a record of employee performance and related processes.
- operate and keep a record of employee absences.
- obtain occupational health advice, to ensure that we comply with our duties in relation to individuals with disabilities and ensure that employees are receiving the pay or other benefits to which they are entitled.
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental leave), to ensure that we comply with our duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled.
- provide references on request for current or former employees.
- respond to and defend against legal claims.
- maintain and promote equality in the workplace.
- to promote our organisation through our website and social media platforms by celebrating achievements.

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes). We are not required to obtain consent for this processing as we so under Article 9 (2.b) GDPR which states "*processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment*".

6.5 Access to Staff Personal Data

Your information will be shared internally with other members of our team when necessary in the performance of their duties and is kept strictly confidential at all times.
Ways in which we may share personal information include:

- with Irish Revenue and any other governmental, statutory and/or regulatory departments and/or agencies.
- to engage external IT providers so as to ensure the security of our IT systems in order to protect all personal data.
- with our insurers or assessors when providing or reviewing information in the event of an incident occurring.
- to engage professional services of third parties, such as auditors, solicitors or any other such business advisers. Any such parties are bound by confidentiality.
- we reserve the right to report to law enforcement any activities that we, in good faith, believe to be illegal.

We do not currently transfer your data to countries outside the European Economic Area

6.6 Data Retention

The retention periods for your personal data are as follows:

Employee Data	**Retention Period**
Payslips and general wages information	3 years
Working hours, name and address of employee, PPS numbers and statements of duties	7 years
Training records	7 years
Records relating to parental leave	8 years

Employee Data	Retention Period
Tax records	7 years
Records relating to workplace accidents	10 years
Employment permit records	7 years or duration of employment

6.7 Your Rights

Under data protection law, you have a number of rights, these include:

- the right to have personal information processed in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- the right to be informed, this means that we need to tell you what data we are using, why we are using it and for what purpose as well as informing you of the details of any third parties in receipt of data from us.
- the right of access, you are allowed to see what data of yours we are processing if you request that from us.
- the right of rectification, that means if the data we are using is incorrect we must correct it.
- the right to erasure (or right to be forgotten), this means that you have the right to issue a request to us requesting the erasure of your personal data. However, in certain cases, under our obligations as an employer, we will have overriding legitimate grounds for continued processing, and we may be unable to comply with such a request.
- the right to restrict processing, this means that you can ask you to stop using your data unless we have a legitimate lawful purpose for continuing to do so.
- the right to data portability, this means that you have the right to move your data to another controller and we must provide you with a copy of your data “in a structured, commonly used and machine-readable format”.
- the right to object, this means that you can object to the use of your data and we must stop using it unless we have an overriding legitimate reason to continue.
- the right not to be subject to automated decision making, including profiling.
- the right to make a complaint; and
- the right to judicial remedy.

Please be aware that these are not absolute rights and restrictions, exemptions and limitations may apply.
If you believe we have not complied with your data protection rights, you can complain to the Data Protection Commission by contacting them through their website www.dataprotection.ie

6.8 Your Responsibilities

In every instance when you are working with another individual’s personal data you must make sure to think at all times about the security of that data, this could be data belonging to another member of staff or data relating to a member, volunteer or any other third party. It is advisable for staff to read the Eventing Ireland’s Data Protection Policy so as to ensure that you follow certain guidelines relating to the security of personal data.

6.9 Guidelines include:

- always ensure that information remains confidential, never disclose or discuss the information you access during the course of your work with any unauthorised parties.
- make sure to use strong passwords, for example a name is not sufficient, passwords should contain upper case and lower-case letters, numbers and special characters and be more than 8 characters in length.
- screens should always be locked, or computers shut down when desks are unattended.
- only store data on approved IT systems.
- do not email data to your personal email account at any time.
- when paper files with personal data on them are not in use they should be stored away securely.

- any hard copies of forms or documents with personal data on them that are not being retained and stored appropriately should be shredded and not disposed of in with regular waste.

6.10 General Working Guidelines:

- Work devices should be used in a safe location, for example in an area to minimise who else can view the screen.
- Lock a device prior to leaving it unattended for any reason.
- Make sure devices are turned off, locked, or stored carefully when not in use.
- Never write down passwords or disclose them to other unauthorised parties.
- Remote any loss or theft of a device immediately.
- All equipment and information must be kept securely; employees should take all necessary steps to ensure that private and confidential material is kept secure at all times and all reasonable precautions are being taken to maintain confidentiality of material in accordance with our requirements.
- If the employee discovers or suspects that there has been an incident involving the security of company information this must be reported immediately to management.
- Any staff you have access to our Social Media accounts must familiarise themselves with our Social Media Usage Guidelines.
- Staff must not setup WhatsApp Groups without first receiving authorisation from the General Manager.
- Any staff responsible for WhatsApp Groups must familiarise themselves with the WhatsApp Usage Guidelines See 4

6.11 IT Specific Guidelines:

- Staff must not download software from the Internet,
- Email attachments from suspicious or unknown sources must not be opened under any circumstances. These emails must be deleted on receipt. Under no circumstances should these files be forwarded to other staff.
- Staff are instructed to always remain alert to the possibility that they may receive phishing emails containing links to malicious websites. Any link contained within an email should not be clicked on unless they have verified the link and the sender.
- Staff must ensure that they do not introduce unauthorised content from disks, memory sticks or any other removable media.
- All viruses detected should be reported immediately.

Reviewed

This Notice is reviewed at least annually, and any updates will be circulated to staff in a timely manner.

DOCUMENT CONTROL	
Document Reference	EI-GDPR POL V.0
Original document Approval Date	November 2023
Revision Date 1.0	November 2024