

Data Protection Policy

*RTIG Library Reference: **RTIGA009-1.0***

28 December 2018

Document price:

Foundation Members:	Free
Full Members:	Free
Associate Members:	Free
Non-members:	Free

© Copyright – RTIG Ltd

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means, electronic, mechanical, photocopying or otherwise without the prior permission of RTIG Ltd

No part of this document or of its contents shall be used by or disclosed to any other party without the express written consent of RTIG Ltd

1 About this document

- 1.1. RTIG collects and uses your personal data only as it is needed for us to deliver to you our products and services.
- 1.2. Our data protection policy is intended to describe to you how and what data we collect, and how and why we use your data. It also describes options for you to access, update or otherwise take control of your personal data.
- 1.3. Appended to the policy are:
 - “Privacy Notice for our Members” describing the specific data we process and legal justification.
 - “Privacy and Cookies Policy” which is used on the website

2 The Policy

- 2.1. RTIG is committed to complying with data protection law and to respecting the privacy rights of individuals. The policy applies to all of our directors, members, and committee (“Members”).
- 2.2. 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.
- 2.3. We recognise that you have an important role to play in achieving these aims. It is your responsibility, therefore, to familiarise yourself with this Policy and to apply and implement its requirements when processing any personal data. *Please pay special attention to sections 16, 17 and 18 as these set out the practical day-to-day actions that you must adhere to when working for and with RTIG.*
- 2.4. Data protection law is a complex area. This Policy has been designed to ensure that you are aware of the legal requirements imposed on you and on us and to give you practical guidance on how to comply with them. This Policy also sets out the consequences of failing to comply with these legal requirements. However, this Policy is not an exhaustive statement of data protection law nor of our or your responsibilities in relation to data protection.
- 2.5. If at any time you have any queries on this Policy, your responsibilities or any aspect of data protection law, seek advice. Contact the RTIG Responsible Person.

3 Who is responsible for data protection?

- 3.1. All our Members are responsible for data protection, and each person has their role to play to make sure that we are compliant with data protection laws.
- 3.2. We are not required to appoint a Data Protection Officer (DPO), we have chosen to appoint a Responsible Person. Details of our current Responsible Person can be found at the end of this policy.

4 Why do we have a data protection policy?

- 4.1. We recognise that processing of individuals' personal data in a careful and respectful manner cultivates trusting relationships with those individuals and trust in our brand. We believe that such relationships will enable our organisation to work more effectively with and to provide a better service to those individuals. #
- 4.2. This Policy works in conjunction with other policies implemented by us from time to time.

5 Status of this Policy and the implications of breach.

- 5.1. Any breaches of this Policy will be viewed very seriously. All Members must read this Policy carefully and make sure they are familiar with it. Breaching this Policy is a disciplinary offence and will be dealt with under our Disciplinary Procedure.
- 5.2. If you do not comply with Data Protection Laws and/or this Policy, then you are encouraged to report this fact immediately to the Responsible Person. 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.
- 5.3. 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 Responsible Person.

6 Other consequences

- 6.1. There are a number of serious consequences for both yourself and us if we do not comply with Data Protection Laws. These include:
- 6.2. For you:
 - Disciplinary action: Where you are a member, failure to comply with our policies could lead to termination of your membership 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.
- 6.3. For the organisation:

- Criminal sanctions: Non-compliance could involve a criminal offence.
- Civil Fines: These can be up to Euro 20 million or 4% of group worldwide turnover whichever is higher.
- Assessments, investigations and enforcement action: We could be assessed or investigated by, and obliged to provide information to, the Information Commissioner on its processes and procedures and/or subject to the Information Commissioner’s powers of entry, inspection and seizure causing disruption and embarrassment.
- Court orders: These may require us to implement measures or take steps in relation to, or cease or refrain from, processing personal data.
- Claims for compensation: Individuals may make claims for damage they have suffered as a result of our non-compliance.
- Bad publicity: Assessments, investigations and enforcement action by, and complaints to, the Information Commissioner quickly become public knowledge and might damage our brand. Court proceedings are public knowledge.
- Loss of business: Prospective members, suppliers, funders and national bodies might not want to deal with us if we are viewed as careless with personal data and disregarding our legal obligations.
- Use of Member time and resources: Dealing with assessments, investigations, enforcement action, complaints, claims, etc takes time and effort and can involve considerable cost.

7 Data protection laws

- 7.1. The Data Protection Act 2018 (“DPA 2018”) applies to any personal data that we process, and then after Brexit the UK will adopt laws equivalent to these Data Protection Laws.
- 7.2. The DPA 2018 requires that the personal data is processed in accordance with the Data Protection Principles (on which see below) and gives individuals rights to access, correct and control how we use their personal data (on which see below).

8 Key words in relation to data protection

- 8.1. 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 a member, supplier, contractor or contact, and that personal data might be written, oral or visual.
- 8.2. 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. if a name or video footage) or might do if taken together with other information available to or obtainable us (e.g. a job title and company name).

- 8.3. Data subject: is the living individual to whom the relevant personal data relates.
- 8.4. Processing: is widely defined under data protection law 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 video images.
- 8.5. 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 Members.
- 8.6. 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 newsletter provider will be a data processor.

9 Personal data

- 9.1. 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 information, training information, 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;
 - 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;
 - 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 meeting is to discuss the individual's behaviour 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; 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).
- 9.2. Information about companies or other legal persons who are not living individuals is not personal data. However, information about directors, shareholders, members and committee members, and about sole traders or partners, is often personal data, so business related information can often be personal data.

9.3. 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;
- Medical and disability information;
- CCTV images;
- Member profile information; and
- Financial information and accounts.

10 Lawful basis for processing

10.1. For personal data to be processed lawfully, we must be processing it on one of the legal grounds set out in the Data Protection Laws.

10.2. For the processing of ordinary personal data in our organisation these may include, among other things:

- the data subject has given their consent to the processing (perhaps on their membership application form or when they registered on the organisation's website)
- the processing is necessary for the performance of a contract with the data subject (for example, for processing membership subscriptions);
- the processing is necessary for compliance with a legal obligation to which the data controller is subject; or
- the processing is necessary for the legitimate interest reasons of the data controller or a third party (for example, keeping in touch with members, access to organisation facilities or providing discounts to 3rd party events).

11 Special category data

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

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

- 11.3. To lawfully process special categories of personal data we must also ensure that either the individual has given their explicit consent to the processing or that another of the following conditions has been met:
- the processing is necessary for the performance of our obligations under employment law;
 - the processing is necessary to protect the vital interests of the data subject. The ICO has previously indicated that this condition is unlikely to be met other than in a life or death or other extreme situation;
 - the processing relates to information manifestly made public by the data subject;
 - the processing is necessary for the purpose of establishing, exercising or defending legal claims; or
 - the processing is necessary for the purpose of venue accessibility.
- 11.4. To lawfully process personal data relating to criminal records and history there are even more limited reasons, and we must either:
- ensure that either the individual has given their explicit consent to the processing; or
 - ensure that our processing of those criminal records history is necessary under a legal requirement imposed upon us.
 - We would normally only expect to process special category personal data or criminal records history data usually in a health and safety context etc.

12 When do we process personal data?

- 12.1. 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.
- 12.2. 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 member files.

13 Outline

- 13.1. 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 these laws.

13.2. In summary, data protection law requires each data controller 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 and processing it fairly and in a transparent manner);
- 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 Members;
- 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 ICO and possibly data subjects where there has been a data breach.

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

13.4. Data protection law in the UK is enforced by the Information Commissioner’s Office (“ICO”). The ICO has extensive powers.

14 Data protection principles

14.1. The Data Protection Laws set out 6 principles for maintaining and protecting personal data, which form the basis of the legislation. All personal data must be:

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

15 Data subject rights

- 15.1. Under Data Protection Laws individuals have certain rights (Rights) in relation to their own personal data. In summary these are:
- The rights to access their personal data, usually referred to as a subject access request
 - The right to have their personal data rectified;
 - The right to have their personal data erased, usually referred to as the right to be forgotten;
 - The right to restrict processing of their personal data;
 - The right to object to receiving direct marketing materials;
 - The right to portability of their personal data;
 - The right to object to processing of their personal data; and
 - The right to not be subject to a decision made solely by automated data processing.
- 15.2. The exercise of these Rights may be made in writing, including email, and also verbally and should be responded to in writing by us (if we are the relevant data controller) without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. We must inform the individual of any such extension within one month of receipt of the request, together with the reasons for the delay.
- 15.3. Where the data subject makes the request by electronic form means, any information is to be provided by electronic means where possible, unless otherwise requested by the individual.
- 15.4. If we receive the request from a third party (e.g. a legal advisor), we must take steps to verify that the request was, in fact, instigated by the individual and that the third party is properly authorised to make the request. This will usually mean contacting the relevant individual directly to verify that the third party is properly authorised to make the request.
- 15.5. There are very specific exemptions or partial exemptions for some of these Rights and not all of them are absolute rights. However the right to not receive marketing material is an absolute right, so this should be complied with immediately.
- 15.6. Where an individual considers that we have not complied with their request e.g. exceeded the time period, they can seek a court order and compensation. If the court agrees with the individual, it will issue a Court Order, to make us comply. The Court can also award compensation. They can also complain to the regulator for privacy legislation, which in our case will usually be the ICO.
- 15.7. In addition to the rights discussed in this document, any person may ask the ICO to assess whether it is likely that any processing of personal data has or is being carried out in compliance with the privacy legislation. The ICO must investigate and may serve an "Information Notice" on us (if we are the relevant data controller). The result of the investigation may lead to an "Enforcement Notice" being issued by the ICO. Any such assessments, information notices or enforcement notices should be sent directly to our Responsible Person from the ICO.
- 15.8. In the event of a Member receiving such a notice, they must immediately pass the communication to our Responsible Person.

16 Notification and response procedure

- 16.1. If a Member has a request or believes they have a request for the exercise of a Right, they should:
- pass the call to the General Manager. The member should take and record all relevant details and explain the procedure. If possible try to get the request confirmed in writing addressed to our Responsible Person; and
 - inform our Responsible Person of the request.
- 16.2. If a letter exercising a Right is received by any Member they should:
- pass the letter to the General Manager;
 - the General Manager must log the receipt of the letter with our Responsible Person and send a copy of it to them; and
 - our Responsible Person will then respond to the data subject on our behalf.
- 16.3. If an email exercising a Rights is received by any Member they should:
- pass the email to the General Manager;
 - the General Manager must log the receipt of the email with our Responsible Person and send a copy of it to them; and
 - our Responsible Person will then respond to the data subject on our behalf.
- 16.4. Our Responsible Person will co-ordinate our response which may include written material provided by external legal advisors. The action taken will depend upon the nature of the request. The Responsible Person will write to the individual and explain the legal situation and whether we will comply with the request. A standard letter/email from the Responsible Person should suffice in most cases.
- 16.5. The Responsible Person will inform the relevant Member(s) of any action that must be taken to legally comply.
- 16.6. The General Manager will be responsible for ensuring that the relevant response is made within the time period required.
- 16.7. The Responsible Person's reply will be validated by the relevant Member responsible for the relevant area of the organisations activity.

17 Your main obligations

- 17.1. 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 the General Manager or the Responsible Person 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 the Responsible Person if you become aware of or suspect the loss of any personal data or any item containing personal data.

18 Your activities

- 18.1. 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.
- 18.2. Areas and activities particularly affected by data protection law include membership, , security (e.g. CCTV), health and safety and treasury.
- 18.3. You must consider what personal data you might handle, consider carefully what data protection law might mean for you and your activities, and ensure that you comply at all times with this policy.

19 Practical matters

- 19.1. 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:
- Never disclose your unique logins and passwords for any of our IT systems 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.
- 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 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 members 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 member or other party in a public place when third parties may overhear, try to limit the information which may identify that person to others who may overhear in a similar way to if you were speaking on the telephone.
- Never act on instructions from someone unless you are absolutely sure of their identity and if you are unsure then take steps to determine their identity. This is particularly so where the instructions relate to information which may be sensitive or damaging if it got into the hands of a third party or where the instructions involve money, valuable goods or items or cannot easily be reversed.
- Do not transfer personal data to any third party without prior written consent of our Responsible Person.
- Do notify the General Manager or our Responsible Person 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 Responsible Person.

19.2. 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 Responsible Person.

20 Foreign transfers of personal data

- 20.1. Personal data must not be transferred outside the European Economic Area (EEA) unless the destination country ensures an adequate level of protection for the rights of the data subject in relation to the processing of personal data or we put in place adequate protections. This is mainly relevant to data held and accessed in Cloud-based services as well as some data processing the organisation may outsource like newsletter processing or data analysis
- 20.2. These protections may come from special contracts we need to put in place with the recipient of the personal data, from them agreeing to be bound by specific data protection rules or due to the fact that the recipients own country's laws provide sufficient protection.
- 20.3. These restrictions also apply to transfers of personal data outside of the EEA even if the personal data is not being transferred outside of the organisation.
- 20.4. You must not under any circumstances transfer any personal data outside of the EEA without the Responsible Person's prior written consent.
- 20.5. We will also need to inform data subjects of any transfer of their personal data outside of the UK and may need to amend their privacy notice to take account of the transfer of data outside of the EEA.
- 20.6. If you are involved in any new processing of personal data which may involve transfer of personal data outside of the EEA, then please seek approval of our Responsible Person prior to implementing any processing of personal data which may have this effect.

21 Queries

- 21.1. If you have any queries about this Policy please contact the Responsible Person.

22 Responsible Person

Tim Rivett
tim.rivett@rtig.org.uk
07479 950850
01226 762712

PRIVACY NOTICE FOR OUR MEMBERS

We are committed to respecting your privacy. This notice is to explain how we may use personal information we collect before, during and after your membership with us. This notice applies to you if you have registered to become or are a member of the organisation. This notice explains how we comply with the law on data protection, what your rights are and for the purposes of data protection we will be the controller of any of your personal information.

References to **we**, **our** or **us** in this privacy notice are to RTIG.

We have appointed a Responsible Person to oversee our compliance with data protection laws and has overall responsibility for data protection compliance. Contact details are set out in the "Contacting us" section at the end of this privacy notice.

1. **PERSONAL INFORMATION WE MAY COLLECT FROM YOU**

Depending on the type of membership you register for with us, you may initially provide us with or we may obtain **personal information** about you, such as information regarding your:

- personal contact details that allows us to contact you directly such as name, title, email addresses and telephone numbers;
- membership start and end date;
- records of your interactions with us such as telephone conversations, emails and other correspondence and your instructions to us;
- any payment details you provide so that we can receive payments from you and details of the financial transactions with you;
- records of your attendance at any events hosted by us;
- images in video and/or photographic form and voice recordings;
- your marketing preferences so that we know whether and how we should contact you.
- any disciplinary and grievance information;

2. **SPECIAL CATEGORIES OF PERSONAL INFORMATION**

We may also collect, store and use the following "**special categories**" of more sensitive personal information regarding you:

- information about your health, including any medical condition, to enable us to provide information in an accessible manner or ensure venues are accessible to you; and

We may not collect all of the above types of special category personal information about you. In relation to the special category personal data that we do process we do so on the basis that

- the processing is necessary for reasons of substantial public interest, on a lawful basis;
- it is necessary for the establishment, exercise or defence of legal claims;
- it is necessary for the purposes of carrying out the obligations and exercising our or your rights in the field of social protection law; or
- based on your explicit consent.

In the table below we refer to these as the “special category reasons for processing of your personal data”.

3. WHERE WE COLLECT YOUR INFORMATION

We typically collect personal information about our members when you apply to become a member of the organisation, you register with us online, when you purchase any services or products we offer, when you make a query and/or complaint or when you correspond with us by phone, e-mail or in some other way.

We may receive personal data about you from a national organisation or Government body as part of providing you the services you receive as a member.

4. USES MADE OF THE INFORMATION

The table below describes the main purposes for which we process your personal information, the categories of your information involved and our lawful basis for being able to do this.

Purpose	Personal information used	Lawful basis
<p>To administer any membership you have with us and managing our relationship with you, including dealing with payments and any support, service or product enquiries made by you</p>	<p>All contact and membership details, transaction and payment information, records of your interactions with us, and marketing preferences.</p>	<p>This is necessary to enable us to properly manage and administer your membership contract with us.</p>

<p>To arrange and manage any contracts for the provision of any services or products</p>	<p>Contact details, transaction and payment information.</p> <p>Records of your interactions with us.</p>	<p>This is necessary to enable us to properly administer and perform any contract for the provision of any services and products you have purchased from us.</p>
<p>To send you information which is included within your membership benefits and any updates on transport technology</p>	<p>Contact and membership details.</p>	<p>This is necessary to enable us to properly manage and administer your membership contract with us.</p>
<p>To send you other marketing information we think you might find useful or which you have requested from us, including our newsletters, information about membership, events and products and information about our partners and national and regional bodies</p>	<p>Contact details and marketing preferences.</p>	<p>Where you have given us your explicit consent to do so.</p>
<p>To answer your queries or complaints</p>	<p>Contact details and records of your interactions with us</p>	<p>We have a legitimate interest to provide complaint handling services to you in case there are any issues with your membership.</p>
<p>Retention of records</p>	<p>All the personal information we collect.</p>	<p>We have a legitimate interest in retaining records whilst they may be required in relation to complaints or claims. We need to retain records in order to properly administer and manage your membership and run the organisation and in some cases we may have legal or regulatory obligations to retain records.</p> <p>We process special category personal data on the basis of the "special category reasons for processing of your personal data" referred to in section 2 above.</p>
<p>The security of our IT systems</p>	<p>Your usage of our IT systems and online portals.</p>	<p>We have a legitimate interest to ensure that our IT systems are secure.</p>

To conduct data analytics studies to better understand event attendance and trends within the sport	Records of your attendance at any events hosted by us.	We have a legitimate interest in doing so to ensure that our membership is targeted and relevant.
For the purposes of promoting the organisation, our events and membership packages.	Images in video and/or photographic form.	Where you have given us your explicit consent to do so.
To comply with health and safety requirements	Records of attendance, CCTV footage and other information obtained through electronic means such as medical information about your health	We have a legal obligation and a legitimate interest to provide you and other members of our organisation with a safe environment in which to participate in events. We process special category personal data on the basis of the "special category reasons for processing of your personal data" referred to in section 2 above.
To administer your attendance at all courses you sign up to.	All contact and membership details, transaction and payment data.	This is necessary to enable us to register you on to and properly manage and administer your attendance on the course and/or programme.
To use information about your physical or mental health (including any injuries) or disability status, to ensure your health and safety and to assess your fitness to participate in any events or activities we host and to provide appropriate adjustments to our facilities.	Health and medical information	We process special category personal data on the basis of the "special category reasons for processing of your personal data" referred to in section 2 above.
To gather evidence for possible grievance or disciplinary hearings	All the personal information we collect	We have a legitimate interest in doing so to provide a safe and fair environment for all members and to ensure the effective management of any disciplinary hearings, appeals and adjudications.

		We process special category personal data on the basis of the "special category reasons for processing of your personal data" referred to in section 2 above.
--	--	---

For some of your personal information you will have a legal, contractual or other requirement or obligation for you to provide us with your personal information. If you do not provide us with the requested personal information we may not be able to admit you as a member or we may not be able to properly perform our contract with you or comply with legal obligations and we may have to terminate your membership. For other personal information you may not be under an obligation to provide it to us, but if you do not provide it then we may not be able to properly perform our contract with you.

Where you have given us your consent to use your personal information in a particular manner, you have the right to withdraw this consent at any time, which you may do by contacting us as described in the "Contacting us" section below.

Please note however that the withdrawal of your consent will not affect any use of the data made before you withdrew your consent and we may still be entitled to hold and process the relevant personal information to the extent that we are entitled to do so on bases other than your consent. Withdrawing consent may also have the same effects as not providing the information in the first place, for example we may no longer be able to provide certain member benefits to you.

5. **DIRECT MARKETING**

Email, post marketing: from time to time, we may contact you by email or post with information about information, products and services we believe you may be interested in.

We will only send marketing messages to you in accordance with the marketing preferences you set. You can then let us know at any time that you do not wish to receive marketing messages by emailing the membership secretary.

6. **DISCLOSURE OF YOUR PERSONAL INFORMATION**

We share personal information with the following parties:

- **Any party approved by you.**
- **Other service providers:** for example, marketing specialists, payment processors, data analysis, access system contractors, promotional advisors, contractors or suppliers and IT services;
- **The Government or our regulators:** where we are required to do so by law or to assist with their investigations or initiatives.
- **Police, law enforcement and security services:** to assist with the investigation and prevention of crime and the protection of national security.

7. **TRANSFERRING YOUR PERSONAL INFORMATION INTERNATIONALLY**

The personal information we collect may be transferred to and stored in countries outside of the UK and the European Union. Some of these jurisdictions require different levels of protection in respect of personal information and, in certain instances, the laws in those countries may be less protective than the jurisdiction you are typically resident in. We will take all reasonable steps to ensure that your personal information is only used in accordance with this privacy notice and applicable data protection laws and is respected and kept secure and where a third party processes your data on our behalf we will put in place appropriate safeguards as required under data protection laws. For further details please contact us by using the details set out in the "Contacting us" section below.

8. **HOW LONG DO WE KEEP PERSONAL INFORMATION FOR?**

The duration for which we retain your personal information will differ depending on the type of information and the reason why we collected it from you. However, in some cases personal information may be retained on a long-term basis: for example, personal information that we need to retain for legal purposes will normally be retained in accordance with usual commercial practice and regulatory requirements. Generally, where there is no legal requirement we retain all physical and electronic records for a period of 6 years after your last contact with us or the end of your membership. Exceptions to this rule are:

- Access records which are held for no more than 12 months unless we need to preserve the records for the purpose of prevention and detection of crime;
- Details regarding unsuccessful membership applicants where we hold records for a period of not more than 24 months;
- Information that may be relevant to personal injury or discrimination claims may be retained until the limitation period for those types of claims has expired. For personal injury or discrimination claims this can be an extended period as the limitation period might not start to run until a long time after the event.

It is important to ensure that the personal information we hold about you is accurate and up-to-date, and you should let us know if anything changes, for example if you change your phone number or email address. You can contact us by using the details set out in the "**Contacting us**" section below.

9. **YOUR RIGHTS IN RELATION TO PERSONAL INFORMATION**

You have the following rights in relation to your personal information:

- the right to be informed about how your personal information is being used;
- the right to access the personal information we hold about you;
- the right to request the correction of inaccurate personal information we hold about you;

- the right to request the erasure of your personal information in certain limited circumstances;
- the right to restrict processing of your personal information where certain requirements are met;
- the right to object to the processing of your personal information;
- the right to request that we transfer elements of your data either to you or another service provider; and
- the right to object to certain automated decision-making processes using your personal information.

You should note that some of these rights, for example the right to require us to transfer your data to another service provider or the right to object to automated decision making, may not apply as they have specific requirements and exemptions which apply to them and they may not apply to personal information recorded and stored by us. For example, we do not use automated decision making in relation to your personal data. However, some have no conditions attached, so your right to withdraw consent or object to processing for direct marketing are absolute rights.

Whilst this privacy notice sets out a general summary of your legal rights in respect of personal information, this is a very complex area of law. More information about your legal rights can be found on the Information Commissioner’s website at <https://ico.org.uk/for-the-public/>.

To exercise any of the above rights, or if you have any questions relating to your rights, please contact us by using the details set out in the "Contacting us" section below.

If you are unhappy with the way we are using your personal information you can also complain to the UK Information Commissioner’s Office or your local data protection regulator. We are here to help and encourage you to contact us to resolve your complaint first.

10. **CHANGES TO THIS NOTICE**

We may update this privacy notice from time to time. When we change this notice in a material way, we will update the version date at the bottom of this page. For significant changes to this notice we will try to give you reasonable notice unless we are prevented from doing so. Where required by law we will seek your consent to changes in the way we use your personal information.

11. **CONTACTING US**

In the event of any query or complaint in connection with the information we hold about you, please email the General Manager in the first instance, or the Responsible Person:

Version dated December 2018

PRIVACY POLICY AND COOKIES POLICY

We at RTIG (“we” or “our” or “us”) want to make sure all the personal information we have collected about you, is safe and secure whether we collect it through our website at rtig.org.uk (“Site”) or from other sources. This Policy set outs our commitments to you, in compliance with and beyond the General Data Protection Regulation (commonly known as the **GDPR**) and explains how we collect, store and use your personal information.

We have appointed a Responsible Person to oversee our compliance with data protection laws. If you have any questions about this Policy or what we do with your personal information, their contact details are set out in the “**Contact**” section below.

PRIVACY NOTICES

Collecting specific, relevant personal information is a necessary part of us being able to provide you with any services you may request from us or in providing services to our customers and members or just managing our relationship with you.

When we hold or use your personal information as a **data controller** (*see below for a description of what this is*) we will provide you with a privacy notice which sets out in detail what information we hold about you (such as your contact details, address, etc.), how your personal information may be used and the reasons for these uses, together with details of your rights.

Where we collect personal information from you directly, we will provide this privacy notice at the time we collect the personal information from you. Where we receive your personal information indirectly, we will provide this privacy notice when we first contact you, first pass the data to someone else or within a month, whichever is the earlier.

We will only provide this privacy notice to you once, generally at the start of our relationship with you. However if the applicable privacy notice is updated substantially, then we may provide you with details of the updated version. You are encouraged to check back regularly for updates.

Please note that it is possible for you to be covered by more than one privacy notice, for example you may be a member who comes attends an event which is recorded. In this example both our member privacy notice and our recording privacy notice would apply to you.

THE DIFFERENCE BETWEEN DATA CONTROLLERS/PROCESSORS

A data controller is a person who controls how personal information is processed and used. A data processor is a person who processes and uses personal information in accordance with the instructions of a third party, i.e. the data controller.

This distinction is important. You have certain rights in relation to your personal information, for example the right to be provided with the personal information held about you and details of its use and the right to have certain of your personal information either erased or anonymised, commonly referred to as the right to be forgotten (*see below to see what rights you have*). These rights can generally only be exercised against a data controller of your information.

In most cases we will be a data controller of your personal information. In any case where we are not a data controller this means that you cannot exercise these rights against us directly (i.e. where we only act as a data processor), but you can do so against the data controller (i.e. the person who controls how we process the personal information). In these cases we will endeavour to inform you who is the data controller of your personal information so that you can direct any such requests to them.

Also it is only a data controller that will provide you with a privacy notice about your personal information, so where we process your personal information as a data controller we will provide you with a privacy notice. Where we process your personal information as a data processor for a third party, that third party should provide you with a privacy notice which will set out details regarding the processing of your personal information, which should also include the processing to be carried out by us on their behalf.

HOW DO WE USE YOUR PERSONAL INFORMATION?

We will use your personal information as described in the privacy notice provided to you, but, for example, we may use your personal information to administer any account(s) you have with us or to send you information we think you have requested or might find useful.

WHO DO WE SHARE YOUR PERSONAL INFORMATION WITH?

Details of how we disclose your personal information are set out in the relevant privacy notice provided to you, but generally it is where we need to do so in order to run the organisation (e.g. where other people process information for us). In such circumstances, we will put in place arrangements to protect your personal information. Outside of that we do not disclose your personal information unless we are required to do so by law.

If we transfer personal information about you outside the European Economic Area (EEA), we will ensure that all reasonable security measures are taken and that any third party processors will be required to process the information in accordance with information protection laws and we will notify you in your privacy notice if we are the information controller.

We do not sell, trade or rent your personal information to others.

HOW LONG DO WE HOLD ON TO YOUR PERSONAL INFORMATION?

Further details of how long we hold onto your personal information for are set out in the relevant privacy notice provided to you, but we will only hold your information for as long as is necessary or where you ask us to delete records we may delete it earlier.

The duration for which we retain your personal information will differ depending on the type of information and the reason why it was collected. However, in some cases personal information may be retained on a long term basis: for example, personal information that we need to retain for legal purposes will normally be retained for at least six years in accordance with usual commercial practice and regulatory requirements.

WHAT ARE YOUR RIGHTS?

Full details of your rights set out in the relevant privacy notice provided to you, but you are entitled by law to ask for a copy of your personal information at any time. You are also entitled to ask us to correct, delete or update your personal information, to send your personal information to you or another organisation and to object to automated decision making. Where you have given us your consent to use your personal information in a particular manner, you also have the right to withdraw this consent at any time.

To exercise any of your rights, or if you have any questions relating to your rights, please contact us by using the details set out in the "**Contact**" section below. You can also unsubscribe from any **direct marketing** by clicking on the unsubscribe link in the marketing messages we send to you.

You should note that some of your rights may not apply as they have specific requirements and exemptions which apply to them and they may not also apply to personal information recorded and stored by us. However your right to withdraw consent or object to processing for direct marketing are absolute rights.

If you are unhappy with the way we are using your personal information you can complain to the UK Information Commissioner's Office or your local data protection regulator. More information about your legal rights can be found on the Information Commissioner's website at <https://ico.org.uk/your-data-matters/>. However, we are here to help and would encourage you to contact us to resolve your complaint first.

LINKING WITH THIRD PARTY SITES

Our Site may, from time to time, contain links to and from the websites of our partners, national bodies and organisations. If you follow a link to any of these websites, please note that these websites have their own privacy policies and they will be a data controller of your personal information. We do not accept any responsibility or liability for these policies and you should check these policies before you submit any personal information to these websites.

In addition, if you linked to this Site from a third-party site, we cannot be responsible for the privacy policies and practices of the owners or operators of that third-party site and recommend that you check the policy of that third party site and contact its owner or operator if you have any concerns or questions.

SECURITY

We employ a variety of technical and organisational measures to keep your personal information safe and to prevent unauthorised access to, or use, or disclosure of it. Unfortunately, no information transmission over the Internet is guaranteed 100% secure nor is any storage of information always 100% secure, but we do take all appropriate steps to protect the security of your personal information.

COOKIES

Certain parts of our Site use "cookies" to keep track of your visit and to help you navigate between sections. A cookie is a small data file that certain websites store on your computer's hard-drive when you visit such websites. Cookies can contain information such as your user ID and the pages you have visited. The only personal information a cookie contains is information that you have personally supplied.

We use cookies on our Site to enable us to deliver content that is specific to your interests and gives us an idea of which parts of the Site you are visiting and to recognise you when you return to the Site. Reading cookies does not give us access to other information on your computer's hard-drive and our Site will not read cookies created by other websites that you have visited.

You may refuse to accept cookies by activating the setting on your browser which allows you to refuse the setting of cookies. If, however, you select this setting you may be unable to access certain parts of the Site. Unless you have adjusted your browser settings so that it will refuse cookies, our system will issue cookies when you access the Site.

Please note providers of third party content may also use cookies over which we have no control. For detailed information on the cookies we use and the purposes for which we use them see the table at the end of the policy.

LOG FILES

In common with most websites, our Site logs various information about visitors, including internet protocol (IP) addresses, browser type, internet service provider (ISP) information, referring / exit pages and date / time stamp.

We may use this information to analyse trends, administer the Site, track your movement around the Site and gather broad demographic information.

CHANGES TO THIS POLICY

Any changes we may make to this Policy in the future will be posted on our Site and, where appropriate, notified to you by e-mail. When we change this Policy in a material way, we will update the version date at the bottom of this page. Please check back frequently to see any updates or changes to this Policy and should you object to any alteration, please contact us as set out in the "**Contact**" section below.

CONTACT

In the event of any query or complaint in connection with the information we hold about you, please email secretariat@rtiq.org.uk

Whilst this privacy policy sets out a general summary of your legal rights in respect of personal information, this is a very complex area of law. More information about your legal rights can be found on the Information Commissioner's website at <https://ico.org.uk/your-data-matters/>.

Version Date: December 2018

Cookie	Name	Purpose	More information
.ASPXANONYMOUS	ASPX	Anonymous Session Cookie	
language	Selected language	Track the language selected	

.DOTNETNUKE	Session Cookie	Tracks the login status of a user.	This is not set until a visitor is logs in to the site
Authentication	Session Cookie	Tracks the login status of a user.	This is not set until a visitor is logs in to the site