

Chepstow Cycling Club

Data Protection Policy

Our Policy

Chepstow Cycling Club (“**Club**”) is committed to complying with data protection law and to respecting the privacy rights of individuals. The policy applies to all of our Committee Members, Officers and Volunteers (such as Ride Leaders) (“**Officers**”).

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.

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 14, 15 and 16 as these set out the practical day to day actions that you must adhere to when working or volunteering for the club.***

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.

If at any time you have any queries on this Policy, your responsibilities or any aspect of data protection law, seek advice by contacting the Club Secretary who has been appointed to be responsible for its data protection compliance.

1. Who is responsible for data protection?

- 1.1 All our Officers are responsible for data protection, and each person has their role to play to make sure that we are compliant with data protection laws.
- 1.2 We are not required to appoint a Data Protection Officer (DPO), however we have still appointed the Club Secretary Role to be responsible for overseeing our compliance with data protection laws.

2. Why do we have a data protection policy?

- 2.1 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.
- 2.2 This Policy works in conjunction with other policies implemented by us from time to time.

3. Status of this Policy and the implications of breach.

- 3.1 Any breaches of this Policy will be viewed very seriously. All Officers must read this Policy carefully and make sure they are familiar with it. Breaching this Policy could be a disciplinary offence and will be dealt with under our Club Constitution.
- 3.2 If you do not comply with Data Protection Laws and/or this Policy, then you are encouraged to report this fact immediately to the Club Secretary. 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.

3.3 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 Club Secretary.

4. Other consequences

4.1 There are a number of serious consequences for both yourself and us if we do not comply with Data Protection Laws. These include:

4.1.1 For you:

4.1.1.1 **Disciplinary action:** If you are a volunteer, failure to comply with our policies could lead to termination of your volunteering position with us.

4.1.1.2 **Criminal sanctions:** Serious breaches could potentially result in criminal liability.

4.1.1.3 **Investigations and interviews:** Your actions could be investigated and you could be interviewed in relation to any non-compliance.

4.1.2 For the organisation:

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

4.1.2.2 **Civil Fines:** These can be significant and could impede the club developing or existing.

4.1.2.3 **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.

4.1.2.4 **Court orders:** These may require us to implement measures or take steps in relation to, or cease or refrain from, processing personal data.

4.1.2.5 **Claims for compensation:** Individuals may make claims for damage they have suffered as a result of our non-compliance.

4.1.2.6 **Bad publicity:** Assessments, investigations and enforcement action by, and complaints to, the Information Commissioner quickly become public knowledge and might damage our club brand. Court proceedings are public knowledge.

4.1.2.7 **Loss of business:** Prospective members, sponsors, local council, sports bodies and kit suppliers might not want to deal with us if we are viewed as careless with personal data and disregarding our legal obligations.

4.1.2.8 **Use of Committee time and resources:** Dealing with assessments, investigations, enforcement action, complaints, claims, etc takes considerable time and effort detracting from the Committees ability to lead the Club.

5. **Data protection laws**

- 5.1 The Data Protection Act 1998 (“**DPA**”) applies to any personal data that we process, and from 25th May 2018 this will be replaced by the General Data Protection Regulation (**GDPR**) and the Data Protection Act 2018 (“**DPA 2018**”) (together “**Data Protection Laws**”) and then after Brexit the UK will adopt laws equivalent to these Data Protection Laws.
- 5.2 This Policy is written as though GDPR and the DPA 2018 are both in force, i.e. it states the position as from 25th May 2018.
- 5.3 The Data Protection Laws all require 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).

6. **Key words in relation to data protection**

- 6.1 **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 an Officer, Member, prospective Member or supplier, and that personal data might be written, oral or visual (e.g. **photograph or Video**).
- 6.2 **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).
- 6.3 **Data subject** is the living individual to whom the relevant personal data relates.
- 6.4 **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 images.
- 6.5 **Data controller** is the person who decides how personal data is used. As the Club uses British Cycling’s online system in respect of personal data relating to our members then British Cycling is the data controller and the Club is regarded as a data processor. However, should the Club wish to use an individual’s personal data for any purpose other than the running of the Club, event or activity, then the Club would need to obtain prior, recorded consent from them and our processing of their data would need to take place outside of the British Cycling system. At this point, the Club would become a data controller and we would have primary responsibility for compliance with data protection legislation including GDPR.
- 6.6 **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 the Club Treasurer sending annual membership reminders to members will be a data processor.

7. **Personal data**

- 7.1 Data will relate to an individual and therefore be their personal data if it:
- 7.1.1 identifies the individual. For instance, names, addresses, telephone numbers and email addresses;
 - 7.1.2 its content is about the individual personally. For instance, medical records, a recording of their actions, or contact details;
 - 7.1.3 relates to property of the individual, for example their home, their bike or other possessions;

- 7.1.4 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;
 - 7.1.5 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;
 - 7.1.6 has the individual as its focus, that is the information relates to the individual personally rather than to some other person or event he/she was involved in;
 - 7.1.7 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;
 - 7.1.8 is an expression of opinion about the individual; or
 - 7.1.9 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).
- 7.2 Information about companies or other legal persons who are not living individuals is not personal data. However, information about directors, shareholders, officers and employees, and about sole traders or partners, is often personal data, so business related information can often be personal data.
- 7.3 Personal that the Club processes and stores is found in the Club's "Data Mapping Activities Document". This is the master repository for documenting our approach to
- 7.3.1 Process – each process the club uses.
 - 7.3.2 System used for processing data – the system that is utilised to process the data in each process.
 - 7.3.3 System used for storing data – the system the Club uses to store the data.
 - 7.3.4 Data processed – what data is processed for that process.
 - 7.3.5 Retention policy – the retention timescale for data used in each process.
 - 7.3.6 Any specific actions or requirements for handling that data.

8. **Lawful basis for processing**

- 8.1 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.
- 8.2 For the processing of ordinary personal data in our organisation these may include, among other things:
 - 8.2.1 the data subject has given their consent to the processing when they registered at British Cycling's website;
 - 8.2.2 the processing is necessary for the performance of a contract with the data subject (for example, for processing membership subscriptions);
 - 8.2.3 the processing is necessary for compliance with a legal obligation to which the data controller is subject; or
 - 8.2.4 the processing is necessary for the legitimate interest reasons of the data controller or a third party (for example, keeping in touch with members with club matters, forthcoming about events or access to club benefits).

9. **Special category data**

- 9.1 Special category data under the Data Protection Laws is personal data relating to an individual's race or ethnic origins, political opinions, health, religious or other beliefs, trade union records, sexual orientation, biometric data and genetic data.
- 9.2 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.
- 9.3 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:
- 9.3.1 the processing is necessary for the performance of our obligations under law (for example to comply with a lawful request by police or investigative authorities);
 - 9.3.2 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;
 - 9.3.3 the processing relates to information manifestly made public by the data subject;
 - 9.3.4 the processing is necessary for the purpose of establishing, exercising or defending legal claims.
- 9.4 To lawfully process personal data relating to criminal records and history there are even more limited reasons, and we must either:
- 9.4.1 ensure that either the individual has given their explicit consent to the processing; or
 - 9.4.2 ensure that our processing of those criminal records history is necessary under a legal requirement imposed upon us.
- 9.5 We would normally only expect to process special category personal data or criminal records history data usually in the context of our Members, Volunteers (e.g. Coaches) for health and safety requirements or safeguarding checks.
- 9.6 **When do we process personal data?**
- 9.7 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.
- 9.8 Examples of processing personal data might include:
- 9.8.1 Using personal data to correspond with members; or
 - 9.8.2 Holding personal data in our databases or documents; and
 - 9.8.3 Recording personal data in personnel or member files; or
 - 9.8.4 Ride registration sheets containing names and next of kin personal data.
- 9.9 Please refer to our "Data Mapping Activities Document" for the most up to date list of personal data processed by the Club.
10. **Outline**
- 10.1 The main themes of the Data Protection Laws are:

- 10.1.1 good practices for handling personal data;
 - 10.1.2 rights for individuals in respect of personal data that data controllers hold on them; and
 - 10.1.3 being able to demonstrate compliance with these laws.
- 10.2 In summary, data protection law requires each data controller to:
- 10.2.1 only process personal data for certain purposes;
 - 10.2.2 process personal data in accordance with the six principles of 'good information handling' (including keeping personal data secure and processing it fairly and in a transparent manner);
 - 10.2.3 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 Officers;
 - 10.2.4 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
 - 10.2.5 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.
- 10.3 Every Officer has an important role to play in achieving these aims. It is your responsibility, therefore, to familiarise yourself with this Policy.
- 10.4 Data protection law in the UK is enforced by the Information Commissioner's Office ("ICO"). The ICO has extensive powers.
- 11. Data protection principles**
- 11.1 The Data Protection Laws set out six principles for maintaining and protecting personal data, which form the basis of the legislation. All personal data must be:
- 11.1.1 processed lawfully, fairly and in a transparent manner and only if certain specified conditions are met;
 - 11.1.2 collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes ("purpose limitation");
 - 11.1.3 adequate and relevant, and limited to what is necessary to the purposes for which it is processed ("data minimisation");
 - 11.1.4 accurate and where necessary kept up to date;
 - 11.1.5 kept for no longer than is necessary for the purpose ("storage limitation");
 - 11.1.6 processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures ("integrity and security").
- 12. Data subject rights**
- 12.1 Under Data Protection Laws individuals have certain rights (**Rights**) in relation to their own personal data. In summary these are:
- 12.1.1 The rights to access their personal data, usually referred to as a subject access request
 - 12.1.2 The right to have their personal data rectified;
 - 12.1.3 The right to have their personal data erased, usually referred to as the right to be forgotten;

- 12.1.4 The right to restrict processing of their personal data;
 - 12.1.5 The right to object to receiving direct marketing materials;
 - 12.1.6 The right to portability of their personal data;
 - 12.1.7 The right to object to processing of their personal data; and
 - 12.1.8 The right to not be subject to a decision made solely by automated data processing.
- 12.2 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.
- 12.3 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.
- 12.4 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.
- 12.5 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.
- 12.6 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.
- 12.7 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 Club Secretary from the ICO.
- 12.8 In the event of an Officer receiving such a notice, they must immediately pass the communication to our Club Secretary in line with the procedure in section 13.
- 13. Notification and response procedure**
- 13.1 If an Officer has a verbal request or believes they have a request for the exercise of a Right, they should:
- 13.1.1 should take and record all relevant details and explain the procedure. If possible try to get the request confirmed in writing addressed to our Club Secretary; and
 - 13.1.2 inform our Club Secretary of the request.
 - 13.1.3 our Club Secretary will then respond to the data subject on our behalf.
- 13.2 If a letter or fax exercising a Right is received by any Officer they should:

- 13.2.1 pass the letter to our Club Secretary; and
- 13.2.2 our Club Secretary will then respond to the data subject on our behalf.
- 13.3 If an email exercising a Rights is received by any Officer they should:
 - 13.3.1 pass the email to our Club Secretary; and
 - 13.3.2 our Club Secretary will then respond to the data subject on our behalf.
- 13.4 Our Club Secretary will co-ordinate our response [which may include written material provided by British Cycling or external legal advisors. The action taken will depend upon the nature of the request. The Club Secretary will write to the individual and explain the legal situation and whether we will comply with the request. A standard letter/email from the Club Secretary should suffice in most cases.
- 13.5 The Club Secretary will inform the Committee of any action that must be taken to legally comply. The Club Secretary will co-ordinate any additional activity required by the Club IT Coordinator to meet the request.
- 13.6 The Club Secretary's reply will be validated by the Club Chair. For more complex cases, the letter/email to be sent will be checked by external legal advisors.

14. **Your main obligations**

- 14.1 What this all means for you can be summarised as follows:
 - 14.1.1 Treat all personal data with respect;
 - 14.1.2 Treat all personal data how you would want your own personal data to be treated;
 - 14.1.3 Immediately notify the Club Secretary 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;
 - 14.1.4 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
 - 14.1.5 Immediately notify the Club Secretary if you become aware of or suspect the loss of any personal data or any item containing personal data.

15. **Your activities**

- 15.1 Data protection laws have different implications in different areas of our Club and for different types of activity, and sometimes these effects can be unexpected.
- 15.2 Areas and activities particularly affected by data protection law include communications between officers (e.g. WhatsApp groups, emails, etc.), event notifications, processing membership, marketing and promotions, health and safety (e.g. accident forms), finance, disciplinary matters, safeguarding, etc.
- 15.3 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.
- 15.4 Please note that you must never use British Cycling systems to send emails marketing products or services, whether offered by you or 3rd parties, unless these are directly connected to the club by way of a registered sponsorship agreement.
- 15.5 Our Club uses the British Cycling Club Management Tool to manage its membership, the members' details are shared with British Cycling and stored on the British Cycling system.

- 15.6 When new members join the Club then members' details can be listed on the system in one of the following ways:
- 15.6.1 The club member already has an account or membership with British Cycling and either asks to have the club listed on their record or purchases a club subscription. They will then appear in our list of club members.
 - 15.6.2 The club member does not already have an account with British Cycling, but creates one during the purchase of a club subscription. They will then appear in our list of club members.
- 15.7 In the above two scenarios you do not need to take any additional actions as the club member is consenting to share their details with both British Cycling and the Club as part of the joining process.
- 15.8 The British Cycling Club Management Tool allows the export of our club member data in full or in the form of a queried report. If you make any export or copy of the information that British Cycling hold on club members (for example, downloading information to give to a coach or volunteer managing a club activity), this data should be limited to only what is absolutely necessary to run the session. The data should be stored securely at all times (remember to password protect files and computers). In the case of paper copies of information, these should always be kept as securely as possible, i.e. they should not be left lying around for anyone to access and should be destroyed after use (shredded, ideally). You must not share exported data with any third party (anyone outside of your club) for any reason and must not use it for marketing purposes unless you have captured the explicit consent of the club member to do so.
- 15.9 When you use the Club Management Tool to send emails or newsletters to members then the content of these emails must only be in respect of running the Club and its activities. You should be careful not to include any personal details of any club members in the mail unless you have their consent to do so.
- 15.10 You must not use email or newsletter functionality to advertise your own or any third party's commercial business unless these are directly connected to the club by way of a registered sponsorship agreement and then such information should only be included if it is relevant and appropriate for club members and it should be made clear to the club member why the information is included. An example would be that, as part their sponsorship of the club, the local bike shop would like to offer club members 10% off all purchases. The approval of use of club emails or newsletters for such a purpose must be agreed by Club Communications Officer for appropriateness for members and the Club Secretary for compliance with this policy.
- 15.11 The club profile section of the British Cycling website allows for us to have a customisable profile page for our club. It is important that you keep data protection in mind when customising this page. The page allows you to show or hide the Club Secretary's address and telephone number; you should only show this information if you have the consent of the Club Secretary. The email address is not displayed on this page; instead, it is hidden and an online web form is used to send messages to that email address, i.e. at no point is the email address visible to the sender. There is also a free text area, "About our Club", in which you must not share any personal information unless you have the express consent of the individual to do so. The club profile also allows you to link to the following websites: your club Website, Facebook, Twitter and Strava. These sites are outside the British Cycling system, so you will need to ensure that the information displayed on them is also compliant with GDPR.

16. Practical matters

16.1 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:

- 16.1.1 Do not take personal data out of the British Cycling or club systems (unless absolutely necessary).
- 16.1.2 Do not disclose your unique logins and passwords for any of our IT systems.

Do not leave any items containing personal data unattended in a public place, e.g. in a café or Committee meeting venue, trackside, etc and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.
- 16.1.3 Do not 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.
- 16.1.4 Do encrypt laptops, mobile devices and removable storage devices containing personal data.
- 16.1.5 Do lock laptops, files, mobile devices and removable storage devices containing personal data away and out of sight when not in use.
- 16.1.6 Do password protect documents and databases containing personal data.
- 16.1.7 Do not use removable storage media to store personal data unless the personal data on the media is encrypted.
- 16.1.8 Do pick up printing from any shared printer and always check to make sure you only have the printed matter that you expect, and no third party's printing appears in the printing.
- 16.1.9 Do 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.
- 16.1.10 Do dispose of any materials containing personal data securely, whether the materials are paper based or electronic.
- 16.1.11 Do be discrete when in public place, e.g. at an event start/end point, café, trackside and 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 or writing down information or referring to written information. If necessary move location or change to a different task.
- 16.1.12 Do ensure that your screen faces away from prying eyes if you are processing personal data, even if you are working at home or your employers office. Personal data should only be accessed and seen by those who need to see it.
- 16.1.13 Do not leave personal data lying around, store it securely.
- 16.1.14 Do take care when speaking on the phone in a public place, 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.
- 16.1.15 When in public place (such as the start of a ride event, Time Trial, trackside or coaching event) and taking down details or instructions from a member

where third parties may overhear, DO 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.

- 16.1.16 Do not 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.
 - 16.1.17 Do not transfer personal data to any third party without prior written consent of or our Club Secretary.
 - 16.1.18 Do notify our Club Secretary immediately of any suspected security breaches or suspected loss of personal data.
 - 16.1.19 Do report to our Club Secretary immediately if any personal data is lost, or any devices or materials containing any personal data are lost.
- 16.2 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 Club Secretary.

17. **Foreign transfers of personal data**

- 17.1 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 risk is mainly relevant to data held and accessed in Cloud-based services associated with software apps that we may subscribe to.
- 17.2 The Club will normally avoid foreign transfers of personal data and therefore not need to invoke any special protections but in the cases that this is unavoidable then the rest of this section applies.
- 17.3 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.
- 17.4 You must not under any circumstances transfer any personal data outside of the EEA without the Club Secretary's prior written consent. (Be aware that this could inadvertently come about if you transfer personal data to your employers email system or a personal cloud)
- 17.5 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.
- 17.6 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 Club Secretary prior to implementing any processing of personal data which may have this effect.

18. **Data Retention**

- 18.1 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 our membership and run our club and in some cases we may have legal or regulatory obligations to retain records.
- 18.2 We process special category personal data on the basis of the "special category reasons for processing of your personal data" referred to in section 9.

- 18.3 Retention of specific data is defined in the Club’s “Data Mapping Activities Document”
- 18.4 Data shall be deleted or destroyed using an appropriate removal method, some best practice is captured in the table below but common sense will be used to determine the best means of destruction:

Media type	Data storage mechanism	Suggested removal methods
Hard disk drives (HDD)	Non-volatile magnetic	Multi Pass Pattern wiping, disintegration or incineration
Solid state disk drives (SSD)	Non-volatile solid state memory	Multi Pass Pattern wiping, disintegration
CD-R/DVD-R	Write once optical	Abrasion, disintegration, incineration
CD-RW/DVD-RW	Write many optical	Abrasion, disintegration, incineration
BD-R	Write once optical	Abrasion, disintegration, incineration
BD-RE	Write many optical	Abrasion, disintegration, incineration
Ultra-Density Optical (UDO)	Write once or write many optical	Abrasion, disintegration, incineration
Flash disk drives and USB	Non-volatile solid state memory	Multi Pass Pattern wiping, Degaussing, disintegration
Paper based	Printed	Micro Cross Cut Shredding, incineration

- 18.5 If in any doubt on retention or data destruction then please contact the Club Secretary for advice.

19. IT Security

- 19.1 Club Officers are appointed according to processes defined in the Club constitution.
- 19.2 Access to Club IT facilities is granted on your appointment.
- 19.3 When your term as a Club Officer ends, for whatever reason, then It is the Club’s policy to remove access rights to IT systems as soon as practicable by the Club IT Officer or other Club Officer. It is your duty to return any club data to the Club Secretary and you have certain obligations under law not to retain or reveal personal data from your term as a Club Officer.

20. Review and Auditing of Compliance to this Policy

- 20.1 It is important that we regularly check we are compliant with this Data Protection Policy and we are compliant with any changes in Legislation.
- 20.2 Once a year an audit of the Club’s compliance with this data policy is to be conducted. The audit will be conducted by the Club Chair and Club Secretary or an independent Committee Officer.
- 20.3 The record of the audit shall be presented to the Committee at the next committee meeting.
- 20.4 Audit actions shall be dealt with promptly and reviewed by the committee at committee meetings.
- 20.5 The record of the audit shall be retained by the Club Secretary in a suitable format so it can be made available for any independent external scrutiny.

21. Staying Compliant with Applicable Legislation

- 21.1 At a period of no more than once a year, the Club Secretary shall investigate any changes in data protection legislation using resources such as the Information Commissioner, British Cycling or Sport & Recreation Alliance.

- 21.2 In the event of any changes the Club Secretary shall update this policy and / or our Data Privacy Notice(s), and / or Club officer role profiles.
- 21.3 Any changes to this policy shall be brought to the attention of the committee members and club officers for re-familiarisation of the policy and to understand impacts on their roles.
22. **Queries**
- 22.1 If you have any queries about this Policy please contact the Club Secretary.