LONDON DYNAMO

OUR PRIVACY POLICY

BRITISH CYCLING

clubmark

1. HOW WE WILL TREAT PERSONAL DATA

1.1 Every person has rights with regard to the way in which their personal data is handled. In the course of its activities, London Dynamo ("the Club") will collect, store and process personal data about members, contacts, suppliers and third parties ("our Data Subjects"). We recognise that the correct and lawful treatment of this data will maintain confidence in the Club and will provide for successful club management.

1.2 In addition to the above, this data protection policy seeks to ensure compliance with Data Protection Law (defined below) and to follow good practice, to protect the rights of our Data Subjects, to protect us from the risks of a data breach and to make us open about how we process individuals' data.

1.3 Our officers are obliged to comply with this policy when processing personal data on the Club's behalf.

2. ABOUT THIS POLICY

2.1 The types of personal data that we may be required to handle include information about our Data Subjects and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 2018, The Privacy and Electronic Communications (EC Directive) Regulations 2003, and the General Data Protection Regulation (Regulation (EU) 2016/679)(together 'Data Protection Law').

2.2 This policy (and any other documents referred to in it) sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by our Data Subjects or other sources.

2.3 The Club may amend this policy at any time.

2.4 This policy has been approved by the Club's committee. It sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2.5 The Chair of the Club is responsible for ensuring compliance with Data Protection Law and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Chair who can be contacted at info@londondynamo.co.uk. The successor as Chair of the Club shall take over responsibility as shall the successor's successor and so on.

3. DEFINITION OF DATA PROTECTION TERMS

3.1 **Data** is information that is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **Data Subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their personal information.

3.3 **Personal data** means data relating to a living individual who can be identified from that data either directly or indirectly. Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour. Personal data has a very broad definition and if in doubt whether a certain set is or is not personal, we can presume it is.

3.4 **Data controllers** are the people who or organisations which determine the purposes for which and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Law. The Club is the data controller of all personal data used in its management.

In some limited circumstances the Club may be considered a data processor, in particular when acting upon strict client instructions, without exercising any discretion in its choices regarding how a Data Subject's personal data is managed.

3.5 **Data users** are those of our officers and other volunteers whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

3.6 **Data processors** include any person or organisation that processes personal data on our behalf and on our instructions. These include suppliers which handle personal data on our behalf, such as cloud-storage providers, contractors and CRM providers.

3.7 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties, such as our contractors.

3.8 **Special category personal data** is data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Special category personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

3.9 **Services** is the provision of cycling services as a cycling club.

4. DATA PROTECTION PRINCIPLES

4.1 Anyone processing personal data must comply with enforceable principles. These provide that personal data must be:

4.1.1 Processed fairly and lawfully.

4.1.2 Processed for limited purposes and in an appropriate way.

4.1.3 Adequate, relevant and not excessive for the purpose.

4.1.4 Accurate.

4.1.5 Not kept longer than necessary for the purpose.

4.1.6 Processed in line with data subjects' rights.

4.1.7 Secure.

4.1.8 Not transferred to people or organisations situated in countries without adequate protection.

4.2 Anyone processing personal data must be able to demonstrate compliance with the above principles.

5. FAIR AND LAWFUL PROCESSING

5.1 Data protection law is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the Data Subject. This law is evolving fairly quickly and new amendments aim at introducing more accountability, more transparency and more control over individuals' rights.

5.2 For personal data to be processed lawfully, it must be processed on the basis of **one of the legal grounds** set out in the Data Protection Act (which are the same as those in the GDPR). For personal data to be processed fairly, it must be processed in accordance with **all of the principles above**. The legal grounds include, among other things, the Data Subject's freely given, specific, informed and unambiguous consent to the processing.

Alternatively, processing can be carried out on the basis that it is necessary for the performance or the negotiation of a contract with the Data Subject, for the compliance with a legal obligation to which the Data Controller is subject, or for the legitimate interest of the Data Controller or the party to whom the data is disclosed. When special category personal data is being processed, additional conditions must be met. When processing personal data as Data Controllers in the course of running the Club, we will ensure that those requirements are met.

6. PROCESSING FOR LIMITED PURPOSES

6.1 In the course of running the Club, we may collect and process the personal data set out in the Schedule to this policy. This may include data we receive directly from a Data Subject (for example, by corresponding with us by phone or email or data we receive from other sources (including, for example, social media, business partners, payment and delivery services)).

6.2 We will only process personal data for the specific purposes set out in the Schedule or for any other purposes specifically permitted by data protection law or required by other law. Processing the same data for a different purpose (e.g. in relation to another member or service) needs to be notified to the Data Subjects.

7. NOTIFYING DATA SUBJECTS

7.1 In light of the transparency requirements, we will always notify our Data Subjects when we first collect their data about:

7.1.1 Our **identity** and contact details.

7.1.2 The **purposes** for processing and the legal basis for processing.

7.1.3 The personal data **recipients** (the specific recipient who will receive communication).

7.1.4 The **period** for which we will keep the personal data.

7.1.5 Their **rights** as data subjects.

7.2 If we receive personal data about a Data Subject from third parties, we will provide the Data Subject with this information as soon as possible thereafter, usually at the first time we correspond. This information is contained in our Privacy Policy, available to all.

8. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

8.1 We will only collect personal data to the extent that it is required for the specific purpose notified to the Data Subject.

8.2 We will only disclose as much personal data as it is necessary for us to provide our Services to our members.

9. ACCURATE DATA

9.1 We will seek to ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

10. TIMELY PROCESSING

10.1 We will not keep personal data for longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required, or that a data subject has requested to be erased.

11. **PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS**

11.1 We will process all personal data in line with Data Subjects' rights, in particular their right to:

11.1.1 Withdraw their consent to processing data at any time for any reason.

11.1.2 Access a copy of their personal data.

11.1.3 Have their inaccurate personal data rectified (if applicable).

11.1.4 Request the restriction of processing of their personal data to specific purposes.

11.1.5 Have their personal data erased and no longer processed ('the right to be forgotten').

11.1.6 Receive a copy of their data for the purposes of transmitting it to another data controller.

12. **DATA SECURITY**

12.1 We take appropriate security measures against unlawful or unauthorised processing of personal data, and against accidental loss of, or damage to, personal data.

12.2 We have in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if the processor complies with data protection law.

12.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

12.3.1 **Confidentiality** means that only people who are authorised to use the data can access it.

12.3.2 **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed;

12.3.3 **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored in the cloud, instead of on individual PCs and tablets.

12.4 Our security procedures include:

12.4.1 **Strong passwords**. Administrative access to personal data on our system is protected by a Google Account sign-in. Member access to their individual accounts is protected by a password of at least 6 characters in length, with up to 255 characters available for enhanced security.

12.4.2 **Secure suppliers** (processors). The suppliers we use to help us perform our Services provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that any processing they do on our behalf meets the requirements of this Regulation and ensures the protection of the rights of the data subject.

12.4.3 **Staying up to date**. We keep our systems up to date with the latest security updates that their manufacturer produces and recommends.

12.5 Our security procedures are further detailed in the Schedule – Information Security.

13. **TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA**

13.1 We only transfer personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

13.1.1 The Data Subject has been informed about the transfer and has given his or her explicit consent.

13.1.2 The country to which the personal data is transferred ensures an adequate level of protection for the Data Subjects' rights and freedoms.

13.1.3 The transfer is necessary for one of the reasons set out in Data Protection Law, including the performance of a contract between us and the Data Subject, or to protect the vital interests of the Data Subject.

13.4.4 The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.

13.2 Subject to the requirements in Clause 13.1 above, personal data we hold may also be processed by our suppliers as data processors operating outside the EEA. Those suppliers may be engaged in, among other things, the fulfilment of contracts with the Data Subject, the processing of payment details and the provision of support services. The suppliers we use to help us perform our Services provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that any processing they do on our behalf meets the requirements of data protection law and ensures the protection of the rights of the Data Subject.

14. **DISCLOSURE AND SHARING OF PERSONAL INFORMATION**

14.1 We share personal data relating to Data Subjects with our Data Subjects for the purpose of fulfilling our contractual arrangements with the latter.

14.2 We may disclose personal data to our suppliers who we use to help us perform our Services, whether or not they are located within the EEA, if they have provided sufficient guarantees to implement appropriate technical and organisational measures in such a manner that any processing they do on our behalf meets the requirements of data protection law and ensures the protection of the rights of the Data Subject.

14.3 We may also disclose personal data we hold to third parties:

14.3.1 In the event that we provide or require any services to/from them; or

14.3.2 If we or substantially all of our assets are amalgamated with another club, in which case personal data we hold will be one of the transferred assets.

14.4 We may become under a duty to disclose or share a Data Subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the Data Subject or other agreements; or to protect our rights, property, or safety of our officers and volunteers, members, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

15. **DEALING WITH DATA SUBJECT RIGHTS ENFORCEMENT REQUESTS**

15.1 As Data Subjects, our Data Subjects must make a formal request for us to enforce any of their rights outlined in Clause 11 above. This must be made in writing. Data Subjects rights requests should be sent to the club Chair. Any other club officer who receives a written request should forward it to the club Chair.

15.2 We will facilitate the exercise of Data Subject rights; however, we will not respond to manifestly unsound or excessive requests and we will first consult the exemptions that apply to rights enforcement.

15.3 If the request is genuine, we must ascertain the identity of the individual requesting his/her rights to be enforced. We must make sure that information is only given to the person who is entitled to it.

15.4 We must provide an initial reply to a rights enforcement request within 30 calendar days of receipt. We can extend that period with 60 further calendar days, after acknowledging receipt of the request to the Data Subject.

15.5 We are not allowed to charge for responding to one-off requests.

16. **CHANGES TO THIS POLICY**

16.1 We reserve the right to change this policy at any time. Where appropriate, we will notify all members and officers of those changes by mail or email.

Policy prepared by: Cubism Law Solicitors, London EC4A 1DE
Policy operational from: April 2019
Next review date: 30 April 2020
Policy approved by: Alexander Bastin

THE SCHEDULE - DATA PROCESSING ACTIVITIES

Type of data	Names and addresses, telephone numbers, email addresses, pictures, date of birth, gender, proof of identity, financial information, emergency contacts, related parties.
Type of data subject	Members, suppliers and partners.
Type of processing	Storing, communicating and sharing.
Purpose of processing	Cycling club management.
Type of recipient to whom personal data is transferred	Suppliers.
Retention period	For the provision of our services and/or as required by law, whichever is the longer.

THE SCHEDULE – INFORMATION SECURITY

General Guidelines

- The only people able to access data covered by this policy should be those who need it for their involvement in managing the Club.
- Data should not be shared informally. When access to confidential information is required, officers and volunteers can request it from the officer or volunteer responsible for the information.
- Club will provide training to all officers and volunteers to help them understand their responsibilities when handling data.
- The Club's officers should keep all data secure, by taking sensible precautions and following the guidelines in this Policy.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the Club or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Officers should request help from the Chair if they are unsure about any aspect of data protection.

Data Use

Personal data is of no value to the Club unless it can make use of it. However, it is when personal data is accessed and used that it can be at a risk of loss, corruption or theft:

- When working with personal data, Officers should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, unless attachments are password-protected.
- Data must be encrypted before being transferred electronically.
- Personal data should not be transferred outside of the European Economic Area without an appropriate safeguard.
- Officers should where possible not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data Storage

These rules describe how and where data should be safely stored.
When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.
These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Officers should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
- Data should be protected by strong passwords, and passwords should never be shared.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be uploaded to approved cloud computing services.
- Servers containing personal data should be sited in a secure location.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the Club's standard backup procedures.
- Data should only be stored directly on laptops or other mobile devices like tablets or smart phones for a limited period and providing that these are password protected and encrypted.
- All servers and computers containing data should be kept updated and protected by appropriate security software and a firewall.