1. POLICY STATEMENT

1.1. Everyone has rights with regard to the way in which their personal data in handled. Personal Data is any information identifying an individual or information relating to a living, identified or identifiable individual (Data Subject) that we can identify - directly or indirectly - from that data alone or in combination with other identifiers we possess or can reasonably access. During the course of our activities we will collect, store and process Personal Data about our customers, members, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2. British Canoeing is committed to a policy of protecting the rights and privacy of individuals in accordance with the Data Protection Laws. The retained EU law version of the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 demand higher transparency and accountability in how British Canoeing manages and uses Personal Data. It also accords new and stronger rights for individuals to understand and control that use than under previous Data Protection laws.

1.3. Data Users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

2. ABOUT THIS POLICY

2.1. The Data Protection Act 2018 (DPA 2018) and the retained EU law version of the General Data Protection Regulation (UK GDPR) (together "Data Protection Laws") apply to any personal data that we process. These Data Protection Laws strengthened and extended the provisions of the Data Protection Act 1998.

2.2. 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).

2.3. The types of personal data that British Canoeing (We) may be required to handle include information about current, past and prospective suppliers, customers, clients, students 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 Laws.

2.4. 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 data subjects or other sources.

2.5. This policy does not form part of any employee's contract of employment we reserve the right to amend this policy at any time. Where appropriate, we will notify employees and key volunteers of those changes by mail or email.

2.6. This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data. This policy should be read in conjunction with the British Canoeing Data Breach Policy, the British Canoeing Data Retention

Policy, the British Canoeing Employee and Key Volunteer Data Processing Policy, as well as the applicable British Canoeing Privacy Notices.

2.7. The Data Protection Officer (DPO) is responsible for ensuring compliance with the Data Protection Laws and with this policy. This post is held by Nancy Squires, Director of Governance (nancy.squires@britishcanoeing.org.uk). 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 DPO.

3. DEFINITION OF DATA PROTECTION TERMS

3.1. Data is information which 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 including for our employees. 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 (or from that data and other information in our possession). Personal data can be factual (for example, a name, address, email address or date of birth) or it can be an opinion about that person, their actions and behaviour.

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 the Data Protection Laws. We are the data controller of all personal data used in our business for our own purposes.

3.5. Data users are those of our employees and key 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 is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on British Canoeing's behalf.

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.

3.8. We may also collect, store and use the "special categories" of more sensitive personal information Special categories includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Special categories of personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

4. DATA PROTECTION PRINCIPLES

4.1. Anyone processing personal data must comply with the eight enforceable principles of good practice. 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 outside the EEA without adequate protection.

5. FAIR AND LAWFUL PROCESSING

5.1. The Data Protection Laws are 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.

5.2. For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Privacy Notices in our Privacy Centre. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance 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 Categories of data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

6. PROCESSING FOR LIMITED PURPOSES

6.1. In the course of our business, we may collect and process the personal data set out in the Privacy Notices in our Privacy Centre. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

6.2. We will only process personal data for the specific purposes set out in the Privacy Notices or for any other purposes specifically permitted by the Data Protection Laws. We will notify those purposes within the Privacy Notice to the data subject when we first collect the data or as soon as possible thereafter.

7. NOTIFYING DATA SUBJECTS

7.1. If we collect personal data directly from data subjects, we will inform them about:

7.1.1. The purpose or purposes for which we intend to process that personal data.
7.1.2. The purpose of purposes for which we intend to process that personal data.

7.1.3. The types of third parties, if any, with which we will share or to which we will disclose that personal data.

7.1.4. The means, if any, with which data subjects can limit our use and disclosure of their personnel data.

7.1.5. Their rights under the Data Protection Laws.

7.1.6. If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

7.2. We will also inform data subjects whose personal data we process that we are the Data Controller with regard to that data, and that the Director of Governance is the DPO.

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(s) notified to the data subject in the Privacy Notice.

9. ACCURATE DATA

9.1. All employees and key volunteers are responsible for checking that any information they provide to the organisation in connection with their employment is accurate and up to date and for informing the organisation of any changes to the information they have provided e.g. changes of address, either at the time of appointment or subsequently. More generally, we will 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 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.

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. Request access to any data held about them by a data controller.

11.1.2. Prevent the processing of their data for direct-marketing purposes.

11.1.3. Ask to have inaccurate data amended

11.1.4. Prevent processing that is likely to cause damage or distress to themselves or anyone else.

12. DATA SECURITY

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

12.2. We will put 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 they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

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 on the British Canoeing's central computer system instead of individual PCs.

12.4. Security procedures include:

12.4.1. Entry controls. Any stranger seen in entry-controlled areas should be reported.
12.4.2. Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
12.4.3. Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
12.4.4. Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
12.4.5. Passwords, encryption of computerised personal data: If it is computerised, the personal data should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

12.5. All employees and key volunteers are responsible for ensuring that any personal data they hold is kept securely and that it is no disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

13. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

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

13.1.1. If the receiver is located in a third country or territory, or is an international organisation, or is in a particular sector in a country or territory, covered by UK 'adequacy regulations'.
13.1.2. The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
13.1.3. The data subject has given their consent.

13.1.4. The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.

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

13.1.6. The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

13.2. Subject to the requirements in clause 13.1 above, personal data we hold may also be processed by employees and/or key volunteers operating outside the UK or EEA who work for us or for one of our suppliers. That employees and key volunteers maybe engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

14. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

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

14.1.1. In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.

14.1.2. If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

14.2. If we are 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 employees, key volunteers, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

14.3. We may also share personal data we hold with selected third parties for the purposes set out in the Privacy Notices.

15. DEALING WITH SUBJECT ACCESS REQUESTS

15.1. Data subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to their Line Manager or the DPO immediately.

15.2. When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

15.2.1. We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

15.2.2. We will suggest that the caller put their request in writing if we are not sure about the caller’s identity and where their identity cannot be checked.

15.2.3. Our employees will refer a request to their Line Manager or the DPO for assistance in difficult situations. British Canoeing will not tolerate any harassment or intimidation of employees carrying out their duties in accordance with this Policy.

16. EMPLOYEES AND KEY VOLUNTEERS MAIN OBLIGATIONS

16.1. This policy will apply to all British Canoeing employees and key volunteers who may be handling data on behalf of British Canoeing.

16.2. What this all means for you as employees and key volunteers can be summarised as follows. You should:

16.2.1. Treat all personal data with respect;
16.2.2. Treat all personal data how you would want your own personal data to be treated;
16.2.3. Immediately notify your line manager or our DPO if any individual says or do anything which gives the appearance of them wanting to invoke any rights in relation to personal data relating to them;
16.2.4. 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
16.2.5. Immediately notify our DPO if you become aware of or suspect the loss of any personal data or any item containing personal data. For more details on this please our separate Data Breach Policy which applies to the whole organisation and can be found on our website.

17. YOUR ACTIVITIES

17.1. 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.

17.2. Areas and activities particularly affected by data protection laws include Human Resources, payroll, security (e.g. CCTV), member/customer support, sales, [data inputting,] marketing and promotions, health and safety, finance, performance and participation.

17.3. You must consider what personal data you might handle, consider carefully what data protection laws might mean for you and your activities, and ensure that you comply at all times with this policy.

18. PRACTICAL MATTERS

18.1. 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 do nots:

18.1.1. Do not take personal data out of the organisation's premises (unless absolutely necessary).
18.1.2. Only disclose your unique logins and passwords for any of our IT systems to authorised personnel (e.g. IT) and not to anyone else.

18.1.3. 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.

18.1.4. 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.

18.1.5. 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.

18.1.6. Do encrypt laptops, mobile devices and removable storage devices containing personal data.

18.1.7. Do lock laptops, files, mobile devices and removable storage devices containing personal data away and out of sight when not in use.

18.1.8. Do password protect documents and databases containing personal data.

18.1.9. Never use removable storage media to store personal data unless the personal data on the media is encrypted.

18.1.10. When picking up printing from any shared printer always check to make sure you only have the printed matter that you expect, and no third party's printing appears in the printing.

18.1.11. 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.

18.1.12. Do dispose of any materials containing personal data securely, whether the materials are paper based or electronic.

18.1.13. When in a public place, e.g. a train or café, be careful as to who might be able to see the information on the screen of any device you are using when you have personal information on display. If necessary move location or change to a different task.

18.1.14. 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.

18.1.15. Do challenge unexpected visitors or employees or key volunteers accessing personal data.

18.1.16. Do not leave personal data lying around, store it securely.

18.1.17. 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.

18.1.18. If taking down details or instructions from a customer in a public place when third parties may overhear, try to limit the information which may identify that person to others who may overhear in a similar way to if you were speaking on the telephone.

18.1.19. 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.

18.1.20. Do not transfer personal data to any third party without prior written consent of your line manager or our DPO.

18.1.21. Do notify your line manager or our DPO immediately of any suspected security breaches or loss of personal data.

18.1.22. If any personal data is lost, or any devices or materials containing any personal data are lost, report it immediately to our DPO.

18.1.23. 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 DPO.

19. BREACHES OF THIS POLICY

19.1. Any breaches of this Policy will be viewed very seriously. All employees and key Volunteers must read this Policy carefully and make sure they are familiar with it.

19.2. There are a number of serious consequences for both yourself and us if we do not comply with data protection laws. These include:

19.3. For you:

19.3.1. **Disciplinary action:** If you are an employee, your terms and conditions of employment require you to comply with our policies. Failure to do so could lead to disciplinary action including dismissal. Where you are a volunteer, failure to comply with our policies could lead to termination of your volunteering position with us or other disciplinary sanctions under our Disciplinary Regulations.

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

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

19.4. For the organisation:

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

19.4.2. **Civil Fines:** These can be up to Euro 20 million or 4% of group worldwide turnover whichever is higher. These amounts are very substantial.

19.4.3. **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.

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

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

19.4.6. **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.

19.4.7. **Use of management time and resources:** Dealing with assessments, investigations, enforcement action, complaints, claims, etc. takes time and effort and can involve considerable cost.

20. QUERIES

20.1. If you have any queries about this Policy please contact either your line manager or our DPO.

20.2. There is also more detail on Data Protection contained within the relevant Privacy Notices. The general Privacy and Cookies Policy on our website and the general British Canoeing Data Protection Policy.