Edinburgh Fencing Club Data Protection Policy

Version: 1.0
Last Reviewed: July 24th, 2021
Next Review: July 1st, 2022

1. Purpose and scope

1.1. This policy sets out the commitment of Edinburgh Fencing Club (EFC) to exercise best practice when processing personal data, to comply with data protection law (including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA)), and to uphold the rights of individuals to privacy.

1.2. This policy applies to all processing of personal data by EFC in the course of its functions and activities.

1.3. Definition of key terms is included at Annex A.

2. Data protection law and principles

2.1. Data protection law governs the processing of personal data by a data controller, or by a data processor on their behalf. It sets out obligations for organisations processing personal data, and rights for individual data subjects. EFC acts as both a data controller and a data processor in the course of its activities.

2.2. The GDPR sets out principles for the processing of personal data. These are that personal data shall be:

- 2.2.1. Processed lawfully, fairly and in a transparent manner in relation to individuals
- 2.2.2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- 2.2.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- 2.2.4. Accurate and, where necessary, kept up to date
- 2.2.5. Kept in a form which permits identification of data subjects for no longer than is necessary
- 2.2.6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

2.3. Further obligations include:

- 2.3.1. Upholding individuals' rights
- 2.3.2. Demonstrating accountability by evidencing compliance with the data protection principles
- 2.3.3. Appropriately safeguarding any transfer of personal data outside the UK

3. Lawfulness, fairness and transparency

3.1. The GDPR sets out the lawful purposes for which personal data may be processed. These are that:

- 3.1.1. The data subject has given their consent.

3.1.2. The processing is necessary for the performance of a contract with the data subject.
3.1.3. The processing is necessary to fulfil a legal obligation on EFC.
3.1.4. The processing is necessary to protect the data subjects' vital interests.
3.1.5. The processing is necessary for the public interest.
3.1.6. The processing is necessary for the legitimate interests of EFC or a third party.

3.2. EFC will process all personal data in line with a lawful purpose and record this purpose in its record of processing.

3.3. EFC will meet its obligations to fair and transparent processing using communications such as the privacy statement on the EFC website and other information provided to individuals at or after the point of data collection. EFC seeks to help individuals understand how it processes their personal data.

4. Special category data

4.1. Data protection legislation defines categories of personal data which require additional conditions to be met in order for their processing to be fair and lawful. EFC will process such data in accordance with the data protection principles, and in accordance with this policy.

5. **Purpose Limitation**

5.1. EFC will process personal data for specified, explicit and limited purposes, and will not further process that data for incompatible purposes. Processing of personal data beyond the purpose for which it was originally collected will be risk assessed to ensure that it complies with the data protection principles and in particular that it is fair and lawful. Details for such justification will be recorded by EFC.

6. **Data minimisation**

6.1. EFC will process personal data which is adequate, relevant and limited to what is necessary for its purpose. Data collection and use will be risk assessed to ensure that excessive or unnecessary data is not processed.

6.2. Anonymisation and pseudonymisation of data will be considered and where appropriate applied to ensure that individuals are identified only where necessary.

7. Accuracy

7.1. EFC will process personal data which it understands to be accurate, complete, up-to-date and relevant to its purpose. Where personal data is found to be inaccurate, that inaccuracy will be addressed prior to further processing, or the data deleted. EFC will take all reasonable steps to ensure that personal data remains accurate over time.

8. Storage limitation

8.1. EFC will retain personal data only for as long as is necessary to its purpose and will apply clearly defined rules governing the retention and disposal of

data (as set out in our Privacy Policy). Destruction of personal data will be carried out securely.

8.2. Where retention beyond these rules is necessary, the reasons for this will be recorded, and steps taken to ensure that personal data is removed or obscured using techniques such as anonymisation or pseudonymisation.

9. Security and data breaches

9.1. EFC will implement appropriate organisational and technical measures to protect personal data against unauthorised or unlawful processing, and against accidental loss, destruction or damage. Such measures will protect the confidentiality, availability and integrity of personal data at all times.

9.2. EFC will continually develop and implement safeguards to protect personal data, apply these consistently, and regularly review their effectiveness. Such safeguards will be proportionate and appropriate to risk, considering sensitivity and volume of data, and potential for damage or distress to data subjects which might result from unauthorised or unlawful processing.

9.3. Safeguards will be designed and implemented taking into account the current state of technology and the evolving nature of threats to personal data in the digital environment.

9.4. EFC will implement policy and procedure for the encryption of data, the application of controls to data access, and the transfer of data beyond EFC.

9.5. EFC will operate appropriate procedures for managing any information security incident which may constitute a personal data breach. Notification of personal data breaches to the ICO and data subjects is legally mandated in certain circumstances. Assessment of data breaches and, where appropriate reporting, is the responsibility of the EFC Club Committee & Trustees.

10. Individuals' rights

10.1. EFC will fulfil its obligations to uphold individuals' rights:

- 10.1.1. To be informed
- 10.1.2. To access personal data
- 10.1.3. To rectification of inaccurate personal data
- 10.1.4. To erasure of personal data
- 10.1.5. To restrict processing of personal data
- 10.1.6. To data portability
- 10.1.7. To object to processing of personal data
- 10.1.8. To protection from automated decision making, including profiling

10.2. EFC will operate procedures to appropriately manage requests received from individuals to exercise their rights; these will be managed by the Club Committee & Trustees.

10.3. Information relating to these rights, and the procedures in place to manage rights requests, will be communicated to all committee members, trustees and volunteers.

11. Accountability

11.1. EFC will put adequate resources and controls in place to ensure and evidence compliance with the data protection principles and data protection law. These will include the maintenance of appropriate consent

documentation and communication of all applicable policies and procedures to all committee members, trustees, volunteers or staff, and regular review of its controls to privacy.

11.2. Procedure for processing activities will be reviewed every year in respect of the processing of special category data.

12. Data sharing and disclosure to third parties

12.1. Personal data will be disclosed to third parties appropriately and governed by data sharing agreements and data processor contracts which will provide for appropriate safeguards. Disclosure will be in line with a specific and lawful purpose which will be identified prior to disclosure.

13. Training and awareness

13.1. EFC will ensure that all its committee members, trustees, volunteers, staff and contractors understand their responsibilities in relation to data protection and privacy by providing regular communication, potentially including training for those working in areas, or undertaking roles, with higher privacy risk.

14. Roles and responsibilities

14.1. All EFC committee members, trustees, volunteers, staff and contractors have responsibilities for data protection and privacy, are bound by the commitments of this policy, and are required to effectively operate the various operational procedures which facilitate its fulfilment in practice.

14.2. The EFC Committee and Trustees are responsible for ensuring that the commitments given in this policy are met.

Annex A – Definitions of Key Terms

Anonymisation – The process of turning data into a form which does not identify individuals and where identification is not likely to take place. This allows for a much wider use of the information.

Data controller - An organisation processing personal data, and which determines the purposes and means of processing that personal data.

Data processor – An organisation processing personal data on behalf of a data controller, acting on their instruction.

Data sharing - The sharing of data, usually personal data, between data controllers, typically on a repeated or regular basis.

Data subject – The ‘natural person’ to whom the personal data relates and who is identifiable from that data.

Disclosure - The sharing or publication of personal information with any organisation or individual. It can also be used to describe the sharing of personal information within an organisation, in a way which would not normally be expected.

Encryption – The process of encoding information or data so that only authorised parties can access it.

Personal data - Information relating to an identifiable person who can be directly or indirectly identified. Includes names, staff number, location data, online identifier (eg IP address) and pseudonymised data.

Processing - The use of personal data in any way – this includes collecting, creating, analysing, copying, storing, transferring, sharing, disclosing, publishing and disposing of personal data.

Pseudonymisation – De-identifying data so that a coded reference or pseudonym is attached to a record to allow the data to be associated with a particular individual without that individual being identified directly. Legally, this data remains personal data.

Special category personal data – types of personal data which require additional safeguards and conditions to be met in order for processing to be fair and lawful. Categories are:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic or biometric data
- Sex life or sexual orientation