Musselburgh Rugby Football Club
GDPR policy

1. Introduction

This Policy sets out the obligations of Musselburgh Rugby Football Club ("the Club") regarding data protection and the rights of Club Members, Visitors and Employees ("data subjects") in respect of their personal data under the General Data Protection Regulation ("the Regulation").

The Regulation defines "personal data" as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by the Club, its employees, agents, contractors, or other parties working on behalf of the Club.

The Club is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. The Data Protection Principles

This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be

a) processed lawfully, fairly, and in a transparent manner in relation to the data subject;
b) collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject;
f) 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.

3. Lawful, Fair, and Transparent Data Processing

The Regulation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The Regulation states that processing of personal data shall be lawful if at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
c) processing is necessary for compliance with a legal obligation to which the controller is subject;
d) processing is necessary to protect the vital interests of the data subject or of another natural person;
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4. **Processed for Specified, Explicit and Legitimate Purposes**

4.1 The Club collects and processes the personal data set out in Part 21 of this Policy. This may include personal data received directly from data subjects (for example, contact details used when a data subject communicates with us) and data received from third parties (for example, HMRC tax codes).
4.2 The Club only processes personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.
4.3 The Club recognising the different characteristics applicable to the differing data subjects and purposes of processing, as set out in Part 21.

The following reasons for processing data apply.

(a) Adult memberships - The Club processes the personal data recognising the Legitimate Interests of the membership, and has completed a Legitimate Interests Assessment - Appendix A.
(b) Adult members assisting with Junior rugby development - In respect of these members completing a Child Protection Disclosure application, a copy of this application will be retained to meet legal obligations.
(c) Junior Memberships - The Club will only process the data of junior members (under age 17) with the consent of the parent or guardian of the child.
(d) Members/Visitors - any accidents, either on the course or in the Clubhouse, will be reported under the Clubs health & safety procedures, with any medical information retained by the Club in the interests of the member/visitor concerned.
(e) Employees - The Club processes the personal data under the contract of employment.

5. Adequate, Relevant and Limited Data Processing

The Club will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part 4, above.

6. Accuracy of Data and Keeping Data Up To Date

The Club aims to ensure that all personal data collected and processed is kept accurate and up-to-date. Data subjects will be reminded annually to advise the Club of any changes to the personal data held in the Club records, and will be encouraged to check and amend their personal details using the Club Hub on the Club website. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

7. Timely Processing

The Club shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay.

8. Secure Processing

The Club shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Parts 22 and 23 of this Policy.

9. **Accountability**

9.1 The Club will not appoint a data protection officer, as defined in the Regulation. 9.2 Club Manager shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

a) The name and details of any applicable third party data controllers and any applicable third party data processors;
b) The purposes for which the Club processes personal data;
c) Details of the categories of personal data collected, held, and processed by the Club; and the categories of data subject to which that personal data relates;
d) Details (and categories) of any third parties that will receive personal data from the Club;
e) Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
f) Details of how long personal data will be retained by the Club; and
g) Detailed descriptions of all technical and organisational measures taken by the Club to ensure the security of personal data.

10. Privacy Impact Assessments

The Club shall carry out Privacy Impact Assessments when and as required under the Regulation. Privacy Impact Assessments shall be overseen by the Club Manager and shall address the following areas of importance:
10.1 The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;
10.2 Details of the legitimate interests being pursued by the Club;
10.3 An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
10.4 An assessment of the risks posed to individual data subjects; and

10.5 Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

11. The Rights of Data Subjects

The Regulation sets out the following rights applicable to data subjects:

a) The right to be informed;

b) The right of access;

c) The right to rectification;

d) The right to erasure (also known as the 'right to be forgotten');

e) The right to restrict processing;

f) The right to data portability;

g) The right to object;

h) Rights with respect to automated decision-making and profiling.

12. Keeping Data Subjects Informed

12.1 The Club shall ensure that the following information is provided to every data subject when personal data is collected:
a) Details of the Club including, but not limited to, the identity of any appointed Data Protection Officer;
b) The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing;
c) Where applicable, the legitimate interests upon which the Club is justifying its collection and processing of the personal data;
d) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
e) Where the personal data is to be transferred to one or more third parties, details of those parties;
f) Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 24 of this Policy for further details concerning such third country data transfers);
g) Details of the length of time the personal data will be held by the Club, normally:- - In the event that a member resigns from the Club, the personal data will be held until the Club Accounts have been completed for the accounting period covering the last subscription payment from the ex-member; - in the event that an employee leaves employment, the personal data will be retained for up to 7 years from the date of leaving employment of the Club.
h) Details of the data subject's rights under the Regulation;
i) Details of the data subject's right to withdraw their consent to the Club's processing of their personal data at any time;
j) Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation);
k) Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;

l) Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

12.2 The information set out above in Part 12.1 shall be provided to the data subject at the following applicable time:

12.2.1 Where the personal data is obtained from the data subject directly, at the time of collection;
12.2.2 Where the personal data is not obtained from the data subject directly (i.e. from another party):
a) If the personal data is used to communicate with the data subject, at the time of the first communication; or
b) If the personal data is to be disclosed to another party, before the personal data is disclosed; or
c) In any event, not more than one month after the time at which the Club obtains the personal data.

13. **Data Subject Access**

13.1 A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which the Club holds about them. The Club is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).
13.2 All subject access requests received must be forwarded to the Club Manager, and data subjects will be advised of the contact details to enable such contact.
13.3 The Club does not charge a fee for the handling of normal SARs. The Club reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. Rectification of Personal Data

14.1 If a data subject informs the Club that personal data held by the Club is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

14.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

15. **Erasure of Personal Data**

15.1 Data subjects may request that the Club erases the personal data it holds about them in the following circumstances:

a) It is no longer necessary for the Club to hold that personal data with respect to the purpose for which it was originally collected or processed. The data subject wishes to withdraw their consent to the Club holding and processing their personal data;
b) The data subject objects to the Club holding and processing their personal data (and there is no overriding legitimate interest to allow the Club to continue doing so) (see Part 18 of this Policy for further details concerning data subjects' rights to object);
c) The personal data has been processed unlawfully;

d) The personal data needs to be erased in order for the Club to comply with a particular legal obligation;

15.2 Unless the Club has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

15.3 In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. Restriction of Personal Data Processing

16.1 Data subjects may request that the Club ceases processing the personal data it holds about them. If a data subject makes such a request, the Club shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.
16.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. **Data Portability**

The Club does not process personal data using automated means.

18. **Objections to Personal Data Processing**

18.1 Data subjects have the right to object to the Club processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling).
18.2 Where a data subject objects to the Club processing their personal data based on its legitimate interests, the Club shall cease such processing forthwith, unless it can be demonstrated that the Club's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.
18.3 Where a data subject objects to the Club processing their personal data for direct marketing purposes, the Club shall cease such processing forthwith.

19. **Automated Decision-Making**

The Club does not use personal data for the purposes of automated decision-making.

20. Profiling

The Club does not use personal data for profiling purposes.

21. Personal Data

The following personal data may be collected, held, and processed by the Club:

Members - to participate in the activities of the Club
a) Full name, gender and date of birth;

b) Contact details including home address, telephone number, mobile number and email address;
c) If submitted, the members photograph to be added onto the Club website;
d) If relevant, a copy of any child protection Disclosure Application;

Employees - within contracts of employment
e) Full name, gender and date of birth;
f) Contact details including home address, telephone number, mobile number and email address;
g) Employees banking details, including bank sort code and bank account number;
h) National Insurance number and HMRC tax codes;
i) Level of personal contributions to the Club's pension scheme

22. Data Protection Measures

The Club shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data

a) All emails containing personal data must be pass word protected.
b) Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely.
c) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
d) Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient.
e) No personal data may be shared informally.
f) All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;
g) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Club or not, without the authorisation of the Club Manager;
h) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time;
i) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;
j) No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Club.
k) All personal data stored electronically should be backed up with backups stored offsite. All backups should be encrypted.
l) All electronic copies of personal data should be stored securely using passwords and data encryption (where available for banking and financial transmissions);
m) All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised.
Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Club, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method

n) Personal data held by the Club will only be used to provide data subjects with information regarding Club services, including events and services which are sub-contracted to a 3rd party, eg the professional shop and clubhouse catering services.

23. Organisational Measures

The Club shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data

a) Office employees, agents, contractors, or other parties working on behalf of the Club shall be made fully aware of both their individual responsibilities and the Club's responsibilities under the Regulation and under this Policy, and shall be provided with a copy of this Policy;
b) Only employees, agents, sub-contractors, or other parties working on behalf of the Club that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Club;
c) Those employees, agents, contractors, or other parties working on behalf of the Club handling personal data will be appropriately trained to do so;
d) All employees, agents, contractors, or other parties working on behalf of the Club handling personal data will be appropriately supervised;
e) Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;
f) The performance of those employees, agents, contractors, or other parties working on behalf of the Club handling personal data shall be regularly evaluated and reviewed;
g) All employees, agents, contractors, or other parties working on behalf of the Club handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract;
h) All agents, contractors, or other parties working on behalf of the Club handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Club arising out of this Policy and the Regulation;
i) Where any agent, contractor or other party working on behalf of the Club handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Club against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.
j) Where the Club operates CCTV, this will be organised and controlled under a separate Club CCTV Policy, and following the guidelines produced by the Information Commissioners Office (as amended from time to time).

24. **Transferring Personal Data to a Country Outside the EEA** (For the purposes of these clauses, EEA means European Economic Area plus UK in the event that the UK leaves the EU.)

a) The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;
b) The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the Regulation); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative

arrangements between public authorities or bodies authorised by the competent supervisory authority;
c) The transfer is made with the informed consent of the relevant data subject(s);
d) The transfer is necessary for the performance of a contract between the data subject and the Club (or for pre-contractual steps taken at the request of the data subject);
e) The transfer is necessary for important public interest reasons;
f) The transfer is necessary for the conduct of legal claims;
g) The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
h) The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

24.1 The Club may from time to time transfer ('transfer' includes making available remotely, or storage) personal data to countries outside of the EEA.

24.2 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies

25. Data Breach Notification

25.1 All personal data breaches must be reported immediately to the Club Manager.

25.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Club Manager must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

25.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 25.2) to the rights and freedoms of data subjects, the data protection officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

25.4 Data breach notifications shall include the following information:

a) The categories and approximate number of data subjects concerned;

b) The categories and approximate number of personal data records concerned;

c) The name and contact details of the Club Manager (or other contact point where more information can be obtained);

d) The likely consequences of the breach;

e) Details of the measures taken, or proposed to be taken, by the Club to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

26. Implementation of Policy

This Policy shall be deemed effective as of 17th May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.