



GDPR AND DATA PROTECTION POLICY

Introduction

- 1 In undertaking the business of Muthill Golf Club (MGC, or 'the Club'), we create, gather, store and process data on a variety of data subjects such as on club members (both potential, current and former), staff, customers/suppliers and members of the public. Our use of personal data ranges from CCTV footage, financial transactions with commercial customers through to the processing of a member's details throughout their membership.
- 2 Some of the data we create/collect and process will be other people's personal and/or sensitive data, i.e. data concerning a data subject's racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health or sexual life.
- 3 As our recording and use of data continues to increase, it is more important than ever that every member of the golf club staff understands the law that exists in relation to data protection and staff responsibilities in ensuring that data is secured and protected in line with the law.
- 4 Data protection is an important part of the club's overall information security arrangements. All information must be handled safely and securely according to agreed policy.
- 5 Data protection legislation has existed in the UK for many years with the Data Protection Act (1998) being the current iteration. In May 2018, new legislation will come into force - the General Data Protection Regulations (GDPR).
- 6 As the Club processes 'personal data' of staff, members and other individuals, it is defined as a Data Controller for the purposes of the GDPR. The Club currently processes personal data strictly in accordance with Data Protection legislation and this will continue to be the case in relation to the GDPR.
- 7 The GDPR applies to all data relating to, and descriptive of, living individuals defined in the Regulations as 'personal data'. Individuals are referred to as 'data subjects'. For further definitions of terms used please see the glossary in section 1 of the Data Protection Guidance Handbook.
- 8 The GDPR places obligations on the Club and the way it handles personal data. In turn the staff and members of the Club have responsibilities to ensure personal data is processed fairly, lawfully and securely. This means that personal data should only be processed if we have a valid condition of processing (e.g. legitimate interests, consent obtained from the data subject, or a contract with them) and we have provided information to the individuals concerned about how and why we are processing their information (i.e. a privacy notice). There are restrictions on what we are allowed to do with personal data such as passing personal information on to third parties, transferring information outside the EU or using it for direct marketing.

- 9 Muthill Golf Club is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data.

Purpose of Policy

- 10 This policy sets out the responsibilities of the Club, its staff and its members to comply fully with the provisions of the GDPR. It is accompanied by a list and links to other, associated policies and a Data Protection Guidance Handbook which provides information and guidance on different aspects of data protection and data security. This policy, its associated policies and the Guidance Handbook form the framework from which staff and members should operate to ensure compliance with data protection legislation.

Scope

- 11 The policy applies to all staff and members, and all items of personal data that are created, collected, stored and/or processed through any activity of Muthill Golf Club.

Background

Data Protection principles

- 12 Muthill Golf Club is required to adhere to the six principles of data protection as laid down in the GDPR, which means that information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. The six principles are:
- a) Personal data shall be processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency').
 - b) Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes. Further processing for archiving, scientific or historical research or statistical purposes is permissible ('purpose limitation').
 - c) Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed ('data minimisation').
 - d) Personal data shall be accurate and where necessary kept up to date ('accuracy').
 - e) Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose ('storage limitation').
 - f) Personal data shall be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Personal Data

- 13 Personal data is information about a living individual, who is identifiable from that information or who could be identified from that information when combined with other data which the club either holds or is likely to obtain. GDPR also refers separately to 'special categories' of personal data which includes particularly sensitive personal information such as health details, racial or ethnic origin or religious beliefs. Further information and guidance on personal data, including a full list of 'special categories' of personal data, is provided in section 3 of the Data Protection Guidance Handbook.
- 14 The definition of 'processing data' includes obtaining/collecting, recording, holding, storing, organising, adapting, aligning, copying, transferring, combining, blocking, erasing and destroying the information or data. It also includes carrying out any operation or set of operations on the information or data, including retrieval, consultation, use and disclosure.

- 15 The club, as data controller, remains responsible for the control of personal data it collects even if that data is later passed onto another organisation or is stored on systems or devices owned by other organisations or individuals (including devices personally owned by members of staff).
- 16 Staff developing new projects or processes or revising existing processes need to take data protection into account as part of this process and may need to carry out a data protection impact assessment.
- 17 In the event that there is a data protection breach this will usually have to be reported to the Information Commissioner's Office no later than 72 hours after the breach is discovered, if appropriate. In the first instance, data protection breaches should be reported to the Club Secretary. muthillgolfclub@btconnect.com

Associated Policies

- 18 The following associated policies should be consulted in conjunction with the Data Protection Policy as appropriate.
- Information Security Policy **(to be created)**
 - Records Management Policy **(to be created)**

Policy

The Policy is set out in the following sections:

- [General](#)
- ii. [Data Security](#)
- iii. [Data Retention](#)
- iv. [Conditions of Processing and Consent](#)
- v. [Privacy Notices](#)
- vi. [Record of Processing Activities](#)
- vii. [Children](#)
- viii. [Subject Access Requests and Data Subject Rights](#)
- ix. [Data Sharing](#)
- x. [Data Protection Impact Assessments and Data Protection by Design](#)
- xi. [Direct Marketing](#)
- xii. [Personal Data Breach](#)
- xiii. [Impact of Non-compliance](#)

i. General

- 19 The Club is responsible for demonstrating compliance with the six data protection principles (see paragraph 12).
- 20 Compliance with the GDPR, and adhering to these principles is the responsibility of all members of the Club. Any deliberate breach of this policy may lead to disciplinary action being taken, access to Club facilities being withdrawn, or even criminal prosecution.
- 21 The Club is required to keep a record of its data processing activities as a summary of the processing and sharing of personal information and the retention and security measures that are in place. For more information about these records see section vi Records of Processing Activities.

- **Data Security**

22 All Club users of personal data must ensure that all personal data they hold is kept securely. They must ensure that it is not disclosed to any unauthorised third party in any form either accidentally or otherwise. Data Security should be undertaken in line with the Information Security Policy. **Link to Information Security Policy.**

- **Data Retention**

23 The Club is responsible for ensuring the appropriate retention periods for the information held and managed, based on the Records Management Policy (**to be developed**). Retention periods will be set based on legal and regulatory requirements, sector and good practice guidance.

24 Personal data must only be kept for the length of time necessary to perform the processing for which it was collected. Once information is no longer needed it should be disposed of securely. Paper records should be shredded or disposed of in confidential waste and electronic records should be permanently deleted.

25 If data is fully anonymised then there are no time limits on storage from a data protection point of view (see paragraph 59).

- **Conditions of Processing and Consent**

26 In order for it to be legal and appropriate for the Club to process personal data at least one of the following conditions must be met:

- a) The data subject has given his or her consent
- b) The processing is required due to a contract
- c) It is necessary due to a legal obligation
- d) It is necessary to protect someone's vital interests (i.e. life or death situation)
- e) It 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) It is necessary for the legitimate interests of the controller or a third party and does not interfere with the rights and freedoms of the data subject.

27 All processing of personal data carried out by the Club must meet one or more of the conditions above. In addition the processing of 'special categories' of personal data requires extra, more stringent, conditions to be met in accordance with Article 9 of the GDPR.

28 Under GDPR the club is able to process personal data under conditions of contract (staff), and contract, legitimate interests (members).

29 Consent is defined as “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she by statement or other clear affirmative action, signifies agreement to the processing of personal data relating to him or her”. The GDPR clarifies that silence, pre-ticked boxes or inactivity does not constitute consent.

30 Anyone who has provided consent has the right to revoke their consent at any time.

31 Further information about obtaining consent can be found in section 5 of the Data Protection Guidance Handbook.

- **Privacy Notices**

32 Under the ‘fair and transparent’ requirements of the first data protection principle, the Club is required to provide data subjects with a ‘privacy notice’ to let them know what it does with their personal data (the main privacy notices for the Club can be viewed at: [**under development - link to GDPR page**]).

33 Privacy notices are published on the Club website and are therefore available to staff and members from their first point of contact with the Club. Any processing of staff or members’ data beyond the scope of the standard privacy notice, or processing of the personal information of any other individuals will mean that a separate privacy notice will need to be provided.

34 Further information on what information should be included in a privacy notice is provided in section 5 of the Data Protection Guidance Handbook.

- **Records of Processing Activities**

35 As a data controller the Club is required to maintain a record of processing activities which covers all the processing of personal data carried out by the Club. Amongst other things this record contains details of why the personal data is being processed, the types of individuals about which information is held, who the personal information is shared with and when personal information is transferred to countries outside the EU. The Club has three Records of Processing activities:

- Staff data (including job applicants and previous staff)
- Members’ personal data
- Data subjects other than staff, members, applicants, and past employees

36 Copies of these records can be found in the Club data register.

37 Staff embarking on new activities involving the use of personal data that is not covered by one of the existing records of processing activities should inform the Club Secretary (muthillgolfclub@btconnect.com) before starting the new activity.

- **Children (definition tbc)**

38 Under GDPR the following restrictions apply to the processing of personal information relating to children:

- Online services offered directly to children require parental consent.
- Any information provided to a child in relation to their rights as a data subject has to be concise, transparent, intelligible and easily accessible, using clear and plain language.
- The use of child data for marketing or for profiling requires specific protection.

39 The Club Secretary (muthillgolfclub@btconnect.com) should be informed if any of the above activities are being contemplated.

- **Subject Access Requests and Data Subject Rights**

40 The GDPR gives data subjects the right to access personal information held about them by the Club. The purpose of a subject access request is to allow individuals to confirm the accuracy of personal data and check the lawfulness of processing to allow them to exercise rights of correction or objection if necessary. However, individuals can request to see any information that the Club holds about them which includes copies of email correspondence referring to them or opinions expressed about them.

41 The Club must respond to all requests for personal information and information will normally be provided free of charge.

42 References are disclosable to the person about whom they are written under the subject access provisions of the GDPR. This includes references received by the Club from external sources and confidential references given and received internally. There is an exemption from disclosure for references written by Club staff and sent externally, however these references would still be accessible to the applicant from the organisation to which the reference was sent.

47 For information about making a subject access request see the website. **Link to GDPR page**
Further information and guidance about handling subject access requests can be found in section 7 of the Data Protection Guidance Handbook.

48 Data subjects have a number of other rights under the GDPR. These include:

- **Right to Object** – Data subjects have the right to object to specific types of processing which includes processing for direct marketing, research or statistical purposes. The data subject needs to demonstrate grounds for objecting to the processing relating to their particular situation except in the case of direct marketing where it is an absolute right (see section [xiii on direct marketing](#)). Online services must offer an automated method of objecting.
- **Right to be forgotten (erasure)** – Individuals have the right to have their data erased in certain situations such as where the data are no longer required for the purpose for which they were collected, the individual withdraws consent or the information is being processed unlawfully.
- **Rights in relation to automated decision making and profiling** – The right relates to automated decisions or profiling that could result in significant affects to an individual. Profiling is the processing of data to evaluate, analyse or predict behaviour or any feature of their behaviour, preferences or identity. Individuals have the right not to be subject to decisions based solely on automated processing. When profiling is used, measures must be put in place to ensure security and reliability of services. Automated decision-taking based on sensitive data can only be done with explicit consent.
- **Right to Rectification** - The right to require a controller to rectify inaccuracies in personal data held about them. In some circumstances, if personal data are incomplete, an individual can require the controller to complete the data, or to record a supplementary statement.
- **Right to Portability** – the data subject has the right to request information about them is provided in a structured, commonly used and machine readable form so it can be sent to another data controller. This only applies to personal data that is processed by automated means (not paper records); to personal data which the data subject has provided to the controller, and only when it is being processed on the basis of consent or a contract.

49 Any requests made to invoke any of the rights above must be dealt with promptly and in any case within one month of receiving the request. Members of staff should consult the Club Secretary (muthillgolfclub@btconnect.com) if any requests like these are received.

- **Data Sharing**

50 Certain conditions need to be met before personal data can be shared with a third party or before an external data processor is used to process data on behalf of the Club.

- 51 As a general rule personal data should not be passed on to third parties, particularly if it involves special categories of personal data but there are certain circumstances when it is permissible.
- Any transfers of personal data must meet the data processing principles, in particular it must be lawful and fair to the data subjects concerned (see paragraph 12)
 - It must meet one of the conditions of processing (see [section iv](#)). Legitimate reasons for transferring data would include:
 - That is was a legal requirement
 - It is **necessary** for the official core business of the Club
 - If no other conditions are met then consent must be obtained from the individuals concerned and appropriate privacy notices provided (see section 5 on Consent & Privacy Notices in the Data Protection Guidance Handbook).
 - The Club is satisfied that the third party will meet all the requirements of GDPR particularly in terms of holding the information securely.
 - Where a third party is processing personal data on behalf of the Club a written contract should be in place. A contract is also advisable when data is being shared for reasons other than data processing so the Club has assurances that GDPR requirements are being met.
- 52 Staff should consult with the Club Secretary (muthillgolfclub@btconnect.com) if they are entering into a new contract that involves the sharing or processing of personal data.
- 53 Staff who receive requests for personal information from third parties such as relatives, police, local councils etc. should consult the section 9 of the Data Protection Guidance Handbook on Requests for Personal Information from Third Parties.

- **Data Protection Impact Assessments and Data Protection by Design**

- 54 Under the GDPR the Club has an obligation to consider the impact on data privacy during all processing activities. This includes implementing appropriate technical and organisational measures to minimise the risk to personal data.

- 55 It is particularly important to consider privacy issues when considering new processing activities or setting up new procedures or systems that involve personal data. GDPR imposes a specify 'privacy by design' requirement emphasising the need to implement appropriate technical and organisational measures during the design stages of a process and throughout the lifecycle of the relevant data processing to ensure that privacy and protection of data is not an after-thought.
- 56 Further information about techniques that can be used to reduce the risks associated with handling personal data including Anonymisation and Pseudonymisation see section 12 of the Data Protection Guidance Handbook on Data Protection by Design and Default.
- 57 For some projects the GDPR **requires** that a Data Protection Impact Assessment (DPIA) is carried out. The types of circumstances when this is required include: those involving processing of large amounts of personal data, where there is automatic processing/profiling, processing of special categories of personal data, or monitoring of publicly assessable areas (i.e. CCTV). The DPIA is a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce risks. Information about when and how to carry out a DPIA can be found in section 11 of the Data Protection Guidance Handbook on Data Protection Impact Assessments.

- **Direct Marketing**

- 58 Direct marketing relates to communication (regardless of media) with respect to advertising or marketing material that is directed to individuals e.g. mail shots for fund raising, advertising membership etc. Individuals must be given the opportunity to remove themselves from lists or databases used for direct marketing purposes. The Club must cease direct marketing activity if an individual requests the marketing to stop.
- 59 Direct marketing must also comply with the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)² which covers marketing via telephone, text and email. For more information about direct marketing and PECR please see section 13 of the Data Protection Guidance Handbook.

- **Personal Data Breach**

- 60 The Club is responsible for ensuring appropriate and proportionate security for the personal data that we hold. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage of the data. The Club makes every effort to avoid personal data breaches, however, it is possible that mistakes will occur on occasions. Examples of personal data breaches include:
- Loss or theft of data or equipment
 - Inappropriate access controls allowing unauthorised use
 - Equipment failure
 - Unauthorised disclosure (e.g. email sent to the incorrect recipient)
 - Human error
 - Hacking attack
- 61 If a data protection breach occurs the Club is **required** in some circumstances to report this as soon as possible to the Information Commissioner's Office, and not later than 72 hours after becoming aware of it.

² The Privacy and Electronic Communications (EC Directive) Regulations 2003 is due to be replaced by a new ePrivacy Regulation probably in 2018

62 If you become aware of a data protection breach you must report it immediately. Details of how to report a breach and the information that will be required are included in section 14 of the Data Protection Guidance Handbook on Personal Data Breaches.

Impact of Non-compliance

63 All staff and members of the Club are required to comply with this GDPR Data Protection Policy, its supporting guidance and the requirements specified in the GDPR. Any member of staff or club member who is found to have made an unauthorised disclosure of personal information or breached the terms of this Policy may be subject to disciplinary action. Staff may also incur criminal liability if they knowingly or recklessly obtain and/or disclose personal information without the consent of the Club i.e. for their own purposes, which are outside the legitimate purposes of the Club.

64 The Club could be fined for non-compliance with the GDPR. There are two tiers of fines depending on the type of infringement. Further information about the fines are in section 15 of the Data Protection Guidance Handbook.

Club Contacts

65 Responsibility for data protection at the club rests with the Club Secretary (muthillgolfclub@btconnect.com).

66 In the first instance all enquiries or requests for further information or guidance relating to data protection should be addressed to the

Club Secretary
Muthill Golf Club
Peat Road,
Muthill, Perthshire
PH5 2DA

email: muthillgolfclub@btconnect.com

Tel: 01764 68152