GDPR DATA PROTECTION GUIDANCE HANDBOOK

Glossary

The following terms are used within the Data Protection Policy and Guidance Handbook:

- **Personal Data** – information relating to an identifiable living person ('**data subject**')
- **Processing** – any operation or set of operations carried out on personal data including recording, organisation, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination, erasure or destruction.
- **Profiling** – automated processing of personal data to evaluate certain personal aspects relating to a person, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, reliability, behaviour or movements.
- **Controller** – organisation, person or other body which alone or jointly with others, determines the purpose and means of processing of personal data.
- **Processor** – organisation, person or other body which processes personal data on behalf of the controller.
- **Third party** – organisation, person or other body, other than the data subject, controller or processor.
- **Consent** – of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- **Personal data breach** – beach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
- **GDPR** – EU General Data Protection Regulations

Personal Data

Personal data is information about a living individual (the data subject), who is identifiable from that information or who could be identified from that information combined with other data which the Club either holds or is likely to obtain. This includes names, contact details, photographs, salary, attendance records, sickness absence, leave, dates of birth, marital status, personal email address, online identifiers, IP addresses etc. Furthermore, any expression of opinion or any intentions regarding a person are also personal data.

The GDPR covers all personal data processed by the Club, irrespective of whether these data are held by individual members of staff in their own separate files (including those held outside the Club site e.g. by staff working at home) or centrally by the Club.

The GDPR separately defines 'special categories of personal data' which relates to the following:

- The racial or ethnic origin of the data subject
- Their political opinions
- Their religious or philosophical beliefs
- Whether they are a member of a trade union
- Their genetic data
- Biometric data used to uniquely identify them
- Their physical or mental health or condition
- Their sex life or sexual orientation

'Special Categories of personal data' can only be processed under limited conditions specified in

Article 9 of GDPR. In the context of the Club this would most often be:

- The individual has given their explicit consent
- There is a legal requirement to process this information such as immigration or equality requirements
- The processing is required for occupational health, absence management or the provision of health or social care services or treatment
- We are processing on the basis of legitimate interests, as defined by GDPR

Whilst not defined in GDPR, there are additional types of personal data which if disclosed could cause significant harm or distress. Examples of these include bank account details, national insurance number, copies of identity documents, date of birth etc.

Key Considerations

Before embarking on any processing personal data, whether that be sharing personal data with a third party, using a new online tool, marketing a new programme or any other action that involves the use of personal data, you should ask yourself the following questions:

- Do we really need to record the information?
- Could anonymised or pseudonymised data be used?
- Do we have a valid justification for processing the data i.e. it is required for a contract or has the data subject given their consent.
- Has the subject been told about the processing i.e. been issued with a privacy notice?
- Are we authorised to collect/store/process the personal data?
- Have we checked with the data subject that the personal data is accurate?
- Are we sure that the personal data will be secure during the process?
- Are we planning to pass personal data on to a third party or transfer the data outside the EU? If so do we have the necessary contracts/permissions in place to do this?
- If we are setting up new systems/processes have the Data Protection by Design and Data Protection Impact Assessment guidelines been followed?
- Are there alternative ways the same objective can be achieved without using or sharing personal data?

If, having considered the points above, you conclude that the processing of personal information is necessary then the information in the following sections will provide more details about the factors that need to be considered and the actions that need to be taken to ensure the processing meets the requirements of GDPR.

Data Security

The level of security required should be assessed against the risks associated with the data being processed. Security should also be assured no matter where or by whom data is stored or processed and throughout the whole procedure, including the transmission of data. Appropriate measures must be taken to protect against unauthorised or unlawful access.

Staff and members should not place personal data off site unless absolutely necessary. If it is necessary to place data off site particular care should be taken to ensure the security of the data. Where information is being held or accessed on a mobile device it should be kept secure at all times with appropriate measures in place to prevent theft or interception of transmission. Where personal data is copied onto a mobile device, additional care is needed to avoid personal data becoming inaccurate over time.

All personal data stored on computer equipment or portable storage media must be deleted beyond retrieval prior to equipment disposal.

Appropriate security measures such as encryption and strong access controls should be used.

See also the separate section 12 on Data Protection by Design.

Consent & Privacy Notices

When is Consent needed?

The GDPR requires that all processing of personal information has a lawful basis. Article 6 of GDPR gives a number of circumstances when processing personal information would be justified. See section iv on Conditions of Processing and Consent in the Data Protection Policy for a full list of the lawful reasons for processing. Consent would be used when there is no other lawful basis. This may be the case if we want to use someone's data in a particularly unexpected or potentially intrusive way, or in a way that is incompatible with what we have already told them we will do with their personal data.

The Club has two main privacy notices, one for staff (**[under development - link to be inserted])** and one for members **([under development - link to be inserted]).** These notices provide details to staff and members about what they can expect the Club to do with their personal information. These privacy notices should cover all types of data processing that are **essential** to manage the relationship the Club has with its staff and members and all that happens to personal data while it is held by the Club. The majority of what the Club does with personal data is necessary to the running of the Club and is done in accordance with the official authority vested in the Club by its Charter and Statutes? and in accordance with the contracts the Club has with its staff and members.

Where the Club is using personal information in a new way that is not already part of the Club's core activities covered by the existing privacy notices, it is likely that we will need to seek consent of the individuals concerned, this includes staff, members or other individuals.

Examples of circumstances when consent would be needed include:

- The use of an **online system or third party organisation** to provide a service to staff or members which includes a requirement to transfer personal details such as staff or member contact details (name, email addresses etc).
- Stories or images of individuals put on the **website** or in publications should have consent.
- Using personal information for **direct marketing** or promotion. GDPR requires that consent is obtained for direct marketing.
- Processing of personal information that includes **special categories** of personal data (sensitive personal data such as religious beliefs, racial or ethnic origin, health conditions, sexual orientation etc) will usually require consent.

In summary if a new activity is proposed that involves the use of personal data it is highly likely that consent will be required.

What is Consent?

GDPR defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." Consent therefore needs

to be explicit requiring a positive opt-in (not opt-out, or pre-ticked boxes) and must offer individuals a genuine choice.

Consent that has been obtained must be documented include details of what the individuals were told and when and how they consented.

Individuals must be told that they have the right to withdraw their consent at any time and how to do this.

Privacy Notices
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 we are doing with their personal data. If we are seeking consent for an activity that is not covered by the main staff and member privacy notices of the Club then a separate privacy notice will need to be provided at the same time as consent is sought.

A Privacy notice should include the following information:

- The identity and contact details for the Club or any other partner organisations and the contact details for the responsible officer.
- The purpose the data will be used for.
- The legal basis for processing (usually consent).
- The identity of other people or organisations who may have access to the data.
- Details of any transfers of data outside the EU.
- The retention period of the data or if this is not possible the criteria used to set this.
- The right to access the data, to object to processing or to withdraw consent.
- The right to complain to the Information Commissioner's Office

A template is included in Appendix 1 to help with the development of a privacy notice but all circumstances are slightly different so the information included in the notice will need to be tailored to the particular circumstance.

If consent is being sought or a privacy notice being prepared in relation to a new activity which could have an impact on the privacy of the individuals concerned then consideration should be given to carrying out a Data Protection Impact Assessment (DPIA). For further information about when and how to do a DPIA please see section 11 on Data Protection Impact Assessments.

Subject Access Requests
Any member of staff receiving a request from an individual for their own personal information should forward this to the Club Secretary as soon as possible (muthillgolfclub@btconnect.com).

The purpose of the Subject Access rights 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. The Club must respond to all requests for personal information. The following points should help when dealing with a request. In most cased requests should be sent to the Club Secretary for response.

- The request can be in **any format** provided it is clear. The information provided needs to be enough that you are satisfied that you know who they are, that they are that person they say

they are, and that the scope of the request is clear

- We should be satisfied about the **identity of the requester** before releasing any information. Proof of identity can be requested if required.

- If the **scope of the request** is not clear then we can asked the requester to be more specific about the activities are areas to which the request relates. You can ask them to provide time periods, names of members of staff who may have dealt with them.

- Information must be provided in a **concise, transparent, intelligible** and easily accessible form using clear language.

- The response should be provided in a commonly used **electronic format**, particularly if the request came in electronically, unless the requester asked for another format. When requested by the data subject the information may be provided orally as long as we are confident about the identity of the data subject.

- Information should be provided within **one month**. If the information requested is particularly complex this can be extended by a further two months but the requester must be informed about the extension within one month and the reasons for the delay explained.
- Information must be provided **free of charge** unless additional copies are requested when a reasonable fee can be charged based on administrative costs.

- Where a request is **manifestly unfounded or excessive**, in particular because of their repetitive character the request may be refused. In this case we have to demonstrate how the request is manifestly unfounded or excessive in character.

- The data subject has the **right to obtain the following information**:
    - Confirmation that personal information about them is being processed
    - A copy of that personal information
    - Details of the purpose of the processing
    - Categories of the personal data concerned e.g. does it include any special categories or sensitive personal information
    - Any recipients or categories of recipients the personal information has been shared with, particularly if these are outside the EU.
    - What safeguards are in place for transfers outwith the EU
    - The period the personal information will be stored for or what the criteria is for determining the period of storage.
    - The existence of the right to request from the controller the correction or deletion of personal data or to restrict or object to the processing of personal data concerning them.
    - The right to lodge a complaint with the Information Commissioner's Office
    - What the source of the personal data is if it has not been collected directly from the data subject.
    - Details of any automated decision-making, including profiling, and meaningful information about the logic involved and the envisaged consequences of such processing for the data subject.

- The following information should be **redacted** or otherwise removed from a response before it is sent:

- Personal information relating to other individuals (unless their permission has been obtained to release it)

For details of how to make a subject access request please visit the website: **link to be inserted**

Data Sharing

Before sharing any personal data with any outside organisation there are a number of things that need to be considered or questions that should be asked.

- Does the data sharing need to take place or could the objective be achieved in other ways?
- Are there any risks involved in sharing the personal data. If there could be, a DPIA should be carried out (see data protection privacy impact assessmentsfor details)?
- Does the sharing involve the transfer of data outside the EU (see transfer of personal data outside the EU for further information)?
- Which condition of processing is being met (see section iv of the Data Protection Policy)?
- Have the data subjects been informed about the transfer via a Privacy Notice (see Consent & Privacy Notices)?
- Are all the data protection principles being adhered to (see paragraph 12 of the GDPR and Data Protection Policy)?
- Is the third party acting as a processor for the Club i.e. acting under the instruction of the Club? If so there **must** be a contract between the Club and the processor.
- Even if the third party is not acting as a data processor there should normally be a contract in place to ensure that the third party is adhering to the data protection principle (e.g. holding the data securely, only keeping the data for as long as is required) and meeting the other legal requirements of GDPR.

Contracts

Data processing contracts or data sharing agreements should contain at least the following information:

- The purpose of the sharing or what processing is being carried out on the data
- The potential recipients or types of recipient and the circumstances in which they will have access
- What data will be shared
- Information about the data quality – accuracy, relevance, usability etc
- Data security
- Retention of the data being shared
- The rights of individuals such as how to make a subject access request or complaint
- Review of effectiveness/termination of the agreement
- Sanctions for failure to comply with the agreement

If you are planning to set up a data sharing or data processing contract you should inform the Club Secretary: muthillgolfclub@btconnect.com

Requests for Personal Information from Third Parties

The Club sometimes receives requests for the personal information on its members and staff from third parties. This section is intended to provide advice to staff on how such requests should be handled to ensure compliance with GDPR.

The Club tells members and staff how their information will be used, and in what circumstances and to whom it may be disclosed, through the relevant member and staff privacy notices ([under development - link to be inserted]).

There are some third parties that can require disclosure of personal data, examples of these are in the table below:

Third Party	**Authorisation for disclosure**
Officers of the Department of Works and Pensions, and Local Authorities	Social Security Administration Act 1992: s.110A, s.109B and s.109C
Health and Safety Executive	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR)
Environmental Health Officers	Public Health (Control of Disease) Act 1984 and the Public Health (Infectious Diseases) Regulations 1988
Child Support Agency (CSA)	Child Support (Information, Evidence and Disclosure) Regulations 1992.
Inland Revenue	Taxes Management Act 1970
Police Officers	With a Court Order
Other third parties	With a Court Order

The Club should not process personal information of individuals in ways that are not covered by our privacy notices, or where there is a legal requirement, without explicit consent.

As a general rule, you should never disclose personal data to anyone other than an employee of the Club with a legitimate work interest in the information, without consent.

HOW TO HANDLE COMMON TYPES OF THIRD PARTY REQUEST

Requests for references or confirming qualifications
The requestor should be advised that we require explicit consent from the individual concerned before we can release information (in relation to members it is important not to confirm whether or not the member has attended the Club prior to consent being obtained).

The consent must be in writing (letter or email) and include sufficient information (full name, address, date of birth, dates and subjects of study/areas or work) to allow us to identify them, and be satisfied as to their identity. A letter should be signed or, for a current member or member of staff, an email from their Club email account will be sufficient evidence of identity.

Requests from the Police or law enforcement officials
The Club is not legally obliged to provide information to the police, unless presented with a court order. However, the Club may choose to release information where the police, or other law enforcement agencies, can demonstrate to our satisfaction that non-release would be likely to prejudice the prevention/detection of crime or apprehension/prosecution of offenders.

The Club will aim to support police investigations where possible. However, the Club is obliged to manage personal information in accordance with GDPR.

Requests from the police should:

- be in writing
- be signed and counter signed, the latter by a senior officer
- be for specific information about a specific individual. While this may not always be the case, the information requested should be relevant and limited.
- state that the personal data requested are required for the stated purposes and that failure to provide the information will, in their opinion, be likely to prejudice the investigation.

The Club Secretary (muthillgolfclub@btconnect.com) should be informed when such requests have been received.

Disclosures required by law
There are circumstances where the Club is legally obliged to disclose information about an individual to a third party if this is required by law, enactment or court order (see table above for examples of these cases).

With such requests, we must ensure that any legal obligation (details of legislation and relevant section) is correctly described by the requestor in writing.

All such requests should be referred to the Club Secretary for advice and validation.

Any objections to processing should be referred to the Club Secretary for advice.

Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is a process whereby potential privacy issues and risks are identified and examined from the perspective of all stakeholders and allows the Club to anticipate and address the likely impacts of new initiatives and put in place measures to minimise or reduce the risks. As the use of technology and the collection and storage of personal data grows, the need to ensure that it is properly managed and maintained increases.

It is a requirement of GDPR that a Data Protection Impact Assessment (DPIA) is carried out in certain circumstances. This section will explain when a DPIA has to be done, how it should be carried out, and what should be taken into consideration as part of the process. The impact assessment covers not only the protection of personal data but broader privacy of individuals and therefore could also be referred to as a Privacy Impact Assessments (PIA).

The procedures in this section are designed to minimise the risk of harm that can be caused by the use or misuse of personal information by addressing data protection and privacy concerns at the design and development stage of a project. Conducting a DPIA should benefit the Club by managing risks, avoiding unnecessary costs, avoiding damage to reputation, ensuring legal obligations are met and improving the relationship with stakeholders.

The term project is used in a broad and flexible way and means any plan or proposal. Examples of the types of projects that need a DPIA are:

- A new IT system storing and accessing personal data
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data
- A new surveillance system such as CCTV
- A new database which consolidates information held by separate parts of an organisation

When does a DPIA need to be done?

A DPIA should be done as part of the initial phase of a project to ensure that risks are identified and taken into account before the problems become embedded in the design and causes higher costs due to making changes at a later stage. Also if there is a change to the risk of processing for an existing project a review should be carried out. In the context of this guidance a project could include the development or enhancement of any activity, function or processing such as a system, database, programme, application, service or scheme. The time and effort put into carrying out the DPIA should be proportionate to the risks.

A DPIA does not have to be conducted as a completely separate exercise and it can be useful to consider privacy issues in a broader policy context such as information security. The DPIA does not necessarily need to start and finish before a project can progress further but it can run alongside the project development process.

The GDPR requires that a DPIA is carried out in the following cases:

- When the processing involves systematic and extensive evaluation of personal information particularly in cases of automatic processing or profiling[1] where decisions are made that could have a significant or legal impact on an individual.
- When processing on a large scale of special categories of data (see template form in Appendix 2 for details of these categories) or data relating to criminal convictions and offences
- The monitoring of a publicly assessable area on a large scale
- Any other cases specified by the Information Commissioner (none currently specified)

The Assessment

It is the responsibility of the person leading the project to carry out a DPIA. As part of the process the Club Secretary must be consulted but it is not necessarily the Club Secretary who carries out the DPIA.

If your project includes the use of any personal data then you should start by completing the screening questions on the DPIA form (Appendix 2). If the answer to all these questions in 'No' then the remainder of the assessment does not need to be completed but the results from the screening questions should be sent to the Club Secretary for recording.

If the response to any of the screening questions is 'Yes' you should go on to complete the remainder of the impact assessment form. Guidance notes are included at the end of the form to help the user ensure that the assessment is properly completed.

The assessment template is split into 8 sections:

- *Project details* – providing a broad overview of the project
- *Details of personal data* – providing details of the types of personal data that will be processed and the justification for this
- *Description of information flows* – how the data will be collected, used, stored and deleted
- *Consultation requirements* – detailing consultation with data subjects or other stakeholders
- *Identification of privacy and related risks* – detailing potential risks
- *Identification of privacy solutions* – what will be done to mitigate the risks
- *Sign off and record of outcomes* – an authorised record of the proposed outcomes
- *Integration of outcomes back into the project plan* – detailing of timing and responsibility for each outcome.

Further information about building privacy into a project during the design stage please see Data Protection by Design and by Default.

Once the risks are identified and outcomes and actions agreed it is important that that person leading the project ensures that the necessary actions are implemented. As the project develops and is embedded the privacy risks should continue to be assessed to ensure that adequate protections remain in place.

Once the DPIA process has been completed the outcomes will be recorded in a register maintained by the Club Secretary. The register will record each risk, explain what action has been taken or will be taken and identify who is responsible for approving and implementing the solution.

Data Protection by Design and Default

Data Protection by design (also called Privacy by design) is an approach to handling personal data that promotes privacy and data protection compliance from the start rather than considered as an after- thought.

All staff and agents of the Club are **required** to apply the data protection by design principles when developing a new project or reviewing existing projects that involves the use or storage of personal data. The guidelines below explain the types of project when this might be relevant, what data protection by design is and what measures can be put in please to protect personal data.

Under GDPR the Club has an obligation to consider data privacy during the initial design stages of a project as well as throughout the lifecycle of the relevant data processing. By imposing a specific 'privacy by design' requirement, the GDPR emphasises the need to implement appropriate technical and organisational measures to ensure that privacy and the protection of data is not an after-thought.

Examples of the types of projects where privacy should be considered include:

- Building new IT systems for storing or accessing personal data
- Developing policies or strategies that have privacy implications
- Embarking on a data sharing initiative
- Using data for new purposes

This section explains the concept of 'data protection by design' and suggests factors that can be taken into consideration to ensure that the privacy of individuals is protected. This should read in conjunction with section 11 on Data Protection Impact Assessments.

In addition to meeting legal requirements taking a proactive approach to privacy will reduce the likelihood of fines or financial losses due to data protection breaches and help build reputation and stakeholder confidence.

What is Privacy by Design?

Privacy by Design is an approach to protecting privacy by embedding it into the design specifications of technologies, business practices and physical infrastructure. This means building in privacy during the design phase of any project.

Seven foundation principles of Privacy by Design were first developed by Dr Ann Cavoukian in the 1990s. These can be summarised as:

1	Use **proactive** rather than reactive measures. Anticipate, identify and prevent privacy invasive events before they happen.
2	Privacy should be the **default** position. Personal data must be automatically protected in any system of business practice, with no action required by the individual to protect their privacy
3	Privacy must be **embedded** and integrated into the design of systems and business practices
4	All legitimate interests and objectives are accommodated in a **positive-sum** manner. Both privacy and security are important, and no unnecessary trade-offs need to be made to achieve both.
5	Security should be **end-to-end** throughout the entire lifecycle of the data. Data should be securely retained as needed and destroyed when no longer needed.
6	Visibility and **transparency** are maintained. Stakeholders should be assured that business practices and technologies are operating according to objectives and subject to independent verification.
7	Respect **user privacy** by keeping the interests of the individual uppermost with strong privacy defaults, appropriate notice and user friendly options.

Process

A Data Protection Impact Assessment (DPIA) (see data protection privacy impact assessments) should be carried out as part of the initial phase of a project or when an existing project is being reviewed. If data protection or privacy implications are identified then measures should be built into the project during the early stages to ensure that risks to privacy are minimised or eliminated.

Below are some examples of measures that can be taken during the project development or review to protect the personal data of individuals, not all these examples will be applicable in all circumstances:

- *Data minimisation* – this includes retention minimisation (only keeping personal data for as long as it is required), collection minimisation (only collecting the personal information that is needed) and use minimisation (only use personal data when it is absolutely required therefore reducing the chance of individuals being identified).

- *Deletion* – Having automated deletion processes for particular personal data to ensure it is flagged for deletion after a particular period.

- *Anonymisation* – The data is held in a form where the individuals are no longer identifiable and it is unlikely that any individuals can be re-identified by combining the data with other data e.g. data matching. The GDPR emphasises that anonymization or pseudonymisation should be used wherever possible particularly in relation to historical or scientific research or for statistical purposes.

- *Pseudonymisation* – The identity of an individual is disguised for instance by replacing identifying fields with artificial identifiers or pseudonyms. When data has been pseudonymised it still retains a level of detail which allows tracking back of the data to its original state. This is in contrast to anonymised data where reverse compilation should be impossible.

- *Synthetic data* – As long as the number of individuals in the dataset is large enough, it is possible to generate a dataset composed entirely of 'fictional' individuals or altered identities that retain the statistical properties of the original dataset.
- *Privacy by Default* – The system is set up so the default settings are the ones that provide maximum protection against privacy risks i.e. technical and organisational measures are put in place to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This may mean that the default position would not allow full functionality of the product, unless the user explicitly chooses it.

- *User Access controls* – The amount of personal data that authorised users have access to should be limited to the information they need to know to fulfil their roles.

- *Data subject Access* - Individuals should be able to access their own personal data and be informed of its use and disclosures. If individual users can't access the systems directly themselves it should be set up in a way that allows data to be collated with ease in order to comply with subject assess requests.

- *User friendly systems* – Privacy related functions should be user friendly. For instance users should be able to easily update their details or extract information that relates.

- *Accuracy* – The design should incorporate checks to ensure accuracy and completeness of data and that it is as up-to-date as is necessary to fulfil the specified purposes.

- *Compliance* – The design should include processes to monitor, evaluate, and verify compliance (e.g. with legal requirements, policies and procedures)

- *State of the art* – State of the art technology and organisation measures should be used where possible, however this needs to be balanced against reasonable costs. Old technology should be replaced where possible and software and patches kept up-to-date. In deciding what measures are appropriate, account should be taken of the nature, scope, context and purposes of processing as well as the risks, likelihood and severity for the rights and freedoms of individuals.

- *Security* – Security measures should include processes for secure destruction, appropriate encryption, and strong access control and logging methods.

- *Suppression of data* – The system should be set up to allow the suppression of data of individuals who have objected to receiving direct marketing or those who want to object to decisions being made about them based on automated processing including profiling. Where appropriate the system should also allow data portability in accordance with the GDPR and the right of individuals to request the transmission of their personal data to another data controller in a machine-readable format.

- *Data processors* – Contracts with data processors need to set out how risk/liability will be apportioned between the parties in relation to implementation of 'privacy by design' and 'privacy by default' requirements.

- *Tenders* – Privacy issues should be considered as part of public tenders.

- *Transfers outside EEA* – Particular consideration should be given to protecting personal data when data is likely to be transferred outside the EEA.

These are some example measure that can be taken and not all of them will be appropriate for every project or system, however, it is likely that most projects will benefit from taking some of the steps outlined above. The DPIA should be used to record the privacy measures that are designed into the project.

Direct Marketing

Direct marketing is the communication to a particular individual of any advertising or marketing material. It is not confined to the advertising or marketing of commercial products or services and includes messages trying to sell goods or services and those promoting an organisation or its values or beliefs. Information promoting Club events or opportunities for members could constitute direct marketing and therefore it is important that the Club is aware of these definitions and regulations particularly when sending out mass communications. This covers all forms of communication including by post, telephone, email and other forms of electronic messages.

It is sometimes difficult to tell the difference between a marketing email and a 'service' email. A service email is a communication that is sent to an individual that facilitates or completes a transaction, whether that is for the sale of goods or services. When trying to identify a service email the following questions should be asked:

- Are we under a legal obligation to send the email?
- Is the email part of the performance of a contract?
- Would the individual be at a disadvantage if they did not receive the email?

If the answer to any of these questions is 'yes' then the email is likely to be more of a services email than a marketing email. For instance an email to a member about an offer of a place on a course, paying fees or how to register would all be examples of service emails.

Marketing emails are those that promote the aims and objectives of the Club such as sale of goods, services or organisational ideals.

Any personal details collected and held for direct marketing purposes must comply with the data protection principles e.g. it is fair and lawful, the information is only used for the purpose it is collected for, the information is kept up-to-date, it is not kept for longer than necessary and is held securely.

The easiest way to ensure compliance with the GDPR requirements governing direct marketing is by obtaining consent when contact details are collected and providing an appropriate privacy notice (see section 5 on Consent & Privacy Notices for more information). The consent must be 'opt-in' and any direct marketing messages should only be sent to those people who have opted in. All subsequent marketing communications that are sent should also contain an option to opt-out with details of how the individual can requests not to receive any further messages. If the Club receives an opt-out request it must comply as soon as possible, there are no exceptions to this.

When requesting consent it is good practice to request consent separately for different forms of communication i.e. whether individuals agree to be contacted via post, telephone or email. This is because the different forms of communication are covered by different legislation.

In addition to GDPR the Privacy and Electronic Communications Regulations 2003 (PECR) regulate in detail the use of electronic communications (any text, voice, sound or image message sent over a public electronic communications network e.g. email, SMS text) as a form of marketing. PECR is due to be replaced shortly by a new ePrivacy Regulation (ePR).

Where direct marketing is communicated by telephone, staff must identify themselves and if requested, provide an address or telephone number on which they can be reached. Where cold-calling for fundraising takes place, details should first be checked against the Telephone Preference Service (TPS). Those receiving calls should be made aware of their right to object to the calls.

There is a small exception to the general opt-in consent rule that is the 'soft opt-in' exception. This is where personal data has been collected in the context of an existing relationship with an individual and the Club limits marketing to providing information on similar services/goods. In this case, the soft opt-in allows organisations to market to these individuals via electronic means without having opt-in consent. However, this can only be relied on if the individual was informed at the point of data collection that the information would be used for marketing purposes and they are given the opportunity to opt-out at that stage and in each subsequent piece of communication.

Personal Data Breaches

A personal data breach is defined in GDPR to mean:

> "a breach of security leading to the accidental or unlawful destruction, loss, unauthorised

disclosure of, or access to, personal data transmitted, stored or otherwise processed;"

The Club makes every effort to avoid personal data breaches, however, it is possible that mistakes will occur on occasions or things will happen that are beyond the Club's control. In these cases it is important that the Club responds appropriately. The Club has a responsibility to deal with the breach immediately and appropriately in order to minimise the impact and prevent recurrence. GDPR also imposes a requirement that most personal data breaches are reported to the Information Commissioner's Office within 72 hours of the Club becoming aware of the breach.

This section of the Handbook sets out the procedures to follow if a personal data breach is identified. All individuals who access, use or manage the Club's information are responsible for following these guidelines and for reporting any data protection breaches that come to their attention.

A personal data breach can occur for a number of reasons some examples of these include:

- Loss or theft of data or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Unauthorised disclosure (e.g. email sent to incorrect recipient or document posted to the wrong address or personal information posted onto the website without consent)
- Human error;
- Unforeseen circumstances such as a fire or flood;
- Hacking attack;
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

The consequences of a personal data breach could be physical, material or moral damage to individuals such as loss of control over their personal data, identity theft or fraud, financial loss, damage to the reputation, or any other economic or social disadvantage to the individual concerned.

Reporting an incident
It is the responsibility of any member of staff, member or other individual who discovers a personal data breach to report it immediately as follows:

Email:muthillgolfclub@btconnect.com
or
During working hours call the Club Secretary on Tel: 01764 681523

On initial contact the reporter should provide details of:

- The exact nature of the breach
- An indication of the seriousness of the breach (the sensitivity of the data breached, the number of individuals whose data may be involved, who may have access to the data)
- If possible what action needs to be taken immediately to mitigate the breach

The Club Secretary/Officer will ask you to provide more detailed follow up information (see Appendix 3 for further details) within 24 hours of the discovery of the breach.

It will be the responsibility of the Club's Club Secretary, or their nominee in their absence, to report the incident to the Information Commissioner's Office within 72 hours of being notified of

the breach, if there is evidence of potential harm to the data subject(s).

The Club Secretary will contact other parties as required. Other Club departments will be notified as appropriate, particularly if the breach involves IT security.

Data Subjects
After a personal data breach is identified, the Club will assess whether the breach will result in a high risk to the rights and freedoms of individuals and if so to let the data subject know about the breach as soon as possible.

The Club Secretary will communicate with the area of the Club responsible for the data that has been breached and discuss the best way of contacting the data subjects concerned and what information the data subjects should be given.

When individuals are notified they should be given specific and clear advice on what they can do to protect themselves and what support and advice is available from the Club. They should be provided with details of who they can contact for further information or to ask questions.

Containment and recovery
Steps should be taken as soon as possible to recover any losses and limit the damage. Steps might include:

- Attempt to recover lost equipment
- Use backups to recover lost, damaged or stolen data
- Change relevant passwords as soon as possible.
- If bank details have been lost/stolen, contacting banks directly for advice on preventing fraudulent use.
- Attempt to retrieve personal data, e.g. recall emails, remove from websites etc

Evaluation and response
Once the incident is contained a review should be conducted into the causes of the breach and the effectiveness of the response. The review should consider the type of data, what protections were in place (e.g. encryption), what happened to the data, whether there could be wider consequences of the breach. If ongoing problems are identified then an action plan should be drawn up to put these right. In the case of the most serious breaches a report will be submitted to the Audit Committee.

The Club Secretary will keep a record of all data breaches including the actions taken to mitigate the breach and the lessons learnt.

In the event that Club is responsible for causing a personal data breach, or not taking appropriate action to prevent a breach, then there could be financial consequences. It is therefore important to make every effort to prevent breaches occurring and if breaches do occur take required actions. More information about the impact of non-compliance can be found in GDPR Fines.

GDPR Fines

Examples of the types of situations when fines can be imposed are provided below.

Fines of up to 20,000,000 euros or up to 4% of global turnover, whichever is higher

- Not complying with the basic principles of processing including conditions of processing
- Not complying with data subject rights

Fines of up to 10,000,000 euros or up to 2% of global turnover, whichever is higher

- Not obtaining the correct consent for processing data
- Failure to implement technical and organisational measure to ensure data protection by design
- Not having correct contracts in place for data processors
- Not maintaining adequate written records
- Failing to report a data breach
- Failure to carry out a privacy impact assessment when required

The level of the fines that could be imposed means there could be serious consequences for the Club does not meet the requirements of the GDPR. Fines are likely to be lower if it can be demonstrated that appropriate measures were in place to try and prevent non-compliance.

If data subjects have suffered either material or immaterial harm as a result of an infringement of GDPR there is also the possibility that a claim could be made for financial compensation.

Appendix 1 – Template for Privacy Notice and obtaining consent

Purpose
[Include details of what we are doing with the personal information and how it will be used. Provide as much information as possible including details of why we would like to use their details in this way and what the positive benefits might be for them. If we are processing special categories of personal data or will be using information for marketing purposes this should be specified].

Third Parties
[If the personal information will be shared with any individuals or organisations outwith the Club details should be provided. If the information will not be shared then it may also be helpful to state this].

Overseas transfers
[If the personal information will be transferred outside the EU details should be provided. If any personal information will be placed on a website this should be stated. Note that many online services have servers that are located outwith the EU. Clarification should be sought from the service provider on whether or not this is the case and if so details should be included in the privacy notice.]

Security
[Give details on how the personal information will be stored and what security measures will be in place. For instance, who will have access to it, will it be encrypted, will it be anonymised or pseudonymised?]

Retention
[Give details of how long the personal information will be kept for. If exact details are not known then the basis on which decisions about retention will be made e.g. one year after the end of the project].

Your rights
You have the right to request to see a copy of the information we hold about you and to request corrections or deletions of the information that is no longer required. If you provide consent for us to use your personal data in the ways outline above you have the right to subsequently withdraw you consent. This can be done using the contact details below.

You have the right to lodge a complaint against the Club regarding data protection issues with the Information Commissioner's Office (https://ico.org.uk/concerns/).

Contact details
If you have any questions relating to this consent form or the way we are planning to use your information please contact:
[Your Name and role]
Muthill Golf Club
Peat Road
Muthill
PH5 2DA
[Your email address/telephone number]
The Club's Club Secretary, is Roger Lees. If you have any questions relating to data protection these can be addressed to: muthillgolfclub@btconnect.com in the first instance.

☐ I consent to the Club processing my personal data for the purposes detailed above.

Signed: ……

Date: ……

Appendix 2 – Data Protection Impact Assessment Form

Project Title:	
Brief description of the project (if a business case already exists this may be attached)**:**	
Name of Responsible person:	**Position:**
Responsible School/Service:	
Timing of the project (start/end dates, duration, as applicable)	
Date form completed:	

PART 1
Screening questions

	Yes	No
Will the project involve the collection of new information about individuals?		
Will the project compel individuals to provide information about themselves?		
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?		
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used for?		
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example the using of biometrics or facial recognition.		
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?		
Is the information about individuals a kind particularly likely to raise privacy concerns or expectations including special categories data? For example, health records, criminal records or other information that people would consider to be particularly private.		
Will the project require you to contact individuals in a way which they may find intrusive?		
Will the project introduce new facilities that might be used by individuals in the institution to gather, process, analyse or share personal information in ways that would previously have required specialist support?		
Will the project involve the processing of personal data by third parties (third parties would include all cloud based services)?		
Will the project expose personal data to elevated levels of security risks?		
Are stakeholders likely to have privacy concerns about the project?		

If the answer to any of the questions above is 'Yes', Part 2 of the DPIA should be completed. Otherwise, just complete this page and submit a copy to the Club Secretary.

PART 2 (see notes at the end for guidance on completing each section)

0100090000038d00000002001c0000000000040000000301080005000000b020000000005000000c0210055a
0e040000002e0118001c000000fb02100007000000000bc020000000001020222537973746 56d0000f08eea1bf
08eea1b01000000f08eea1bdc1352fffffffff040000002d010000040000002d0100000400000002010100 1c000000
fb02a4ff000000000000090010000000004400022436 16c6962726900000000000000000000000000000000000000000
0000000000000040000002d010100040000002d010100040000002d010100050000000902000000020d0000003
20a57000000010004000000000550e0e052000360005000000090200000002040000002d010000040000002d0
10000030000000000

0100090000038d00000002001c0000000000040000000301080005000000b020000000005000000c0210055a
0e040000002e0118001c000000fb02100007000000000bc020000000001020222537973746 56d0000f08eea1bf
08eea1b01000000f08eea1bdc1352fffffffff040000002d010000040000002d0100000400000002010100 1c000000
fb02a4ff000000000000090010000000004400022436 16c6962726900000000000000000000000000000000000000000
0000000000000040000002d010100040000002d010100040000002d010100050000000902000000020d0000003
20a57000000010004000000000550e0e052000360005000000090200000002040000002d010000040000002d0
10000030000000000

0100090000038d00000002001c0000000000040000000301080005000000b020000000050000000c0210055a0e
040000002e0118001c000000fb02100007000000000bc020000000001020222537973746 56d0000f08eea1bf08ee
a1b01000000f08eea1bdc1352fffffffff040000002d010000040000002d0100000400000020101001c000000fb02a
4ff000000000000900100000000044000224361 6c6962726900000000000000000000000000000000000000000000000000
0000000040000002d010100040000002d010100040000002d010100050000000902000000020d000000320a5700
0000010004000000000550e0e052000360005000000090200000002040000002d010000040000002d010000030
000000000

0100090000038d00000002001c0000000000040000000301080005000000b020000000050000000c0210055a0e
040000002e0118001c000000fb02100007000000000bc020000000001020222537973746 56d0000f08eea1bf08ee
a1b01000000f08eea1bdc1352fffffffff040000002d010000040000002d0100000400000020101001c000000fb02a
4ff000000000000900100000000044000224361 6c6962726900000000000000000000000000000000000000000000000000
0000000040000002d010100040000002d010100040000002d010100050000000902000000020d000000320a5700
0000010004000000000550e0e052000360005000000090200000002040000002d010000040000002d010000030
000000000

---

5) Identification of privacy and related risks Identify the key privacy risks and associated compliance and corporate risks. Consider whether anything needs to be added to institutional risk registers.			
Privacy issue	Risk to individuals	Compliance risk	Associated organisation/ corporate

6) Identification of privacy solutions Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing systems)			
Risk	Solution(s)	Result: is the risk eliminated, reduced or accepted?	Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the

7) Sign off and record the outcomes		
Risk	Approved solution	Approved by

8) Integrate the outcomes back into the project plan Who is responsible for integrating the outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the		
Action to be taken	Date for completion of actions	Responsibility for action

Please submit a copy of the completed form to the Club Secretary, Roger Lees at muthillgolfclub@btconnect.com

Notes for completing form

1) Project details

Identify why the project is being planned, what the project is intending to achieve and why it is necessary. As well as providing a clear case for the project as a whole, it should highlight those features that may have the potential to impact on privacy. If other organisations are involved in the processing please say who they are and what their involvement is.

2) Details of personal data

Provide details of the personal data involved, including whether it includes special categories of personal data or other sensitive data. Also provide details of the justification for processing the personal data.

3) Describing the information flows

Describe the information flows of the project, how information is collected, stored, used and deleted. How will data be checked for accuracy and kept up to date. Explain what information is used, what it is used for, who it is obtained from and disclosed to, who will have access, and any other necessary information. If the project involves new links with personal data held in other systems please explain. What security measures will be in place? Will any information be sent off site or transferred outside of the EEA? How will individuals be told about the use of their personal data?

4) Consultation requirements

Consultation allows people to highlight privacy risks based on their own area of interest or expertise. It also provides an opportunity for them to suggest measures to reduce the risks. Relevant internal stakeholders should be consulted whilst ensuring their attention is focused on privacy issues. In some cases external consultation may be appropriate. Consultation should be timely, clear, proportionate, reach representative individuals, ask objective questions and seek feedback.

5) Identification of privacy and related risks

Examples of risks include inaccurate, insufficient or out of date information; excessive or irrelevant data; information kept for too long; disclosing the information to someone who should not see it; using information in a way that is unacceptable or unexpected to the person it is about; and information not kept securely. These could cause upset or unnecessary intrusion on privacy. Risks can include risks to physical safety, financial loss or distress caused. Sharing or merging datasets allows the collection of much wider information than an individual might expect.

Some risks will be to the organisation – for example damage to reputation, or the financial costs or a data breach.

Legal compliance risks include the EU General Data Protection Regulations (GDPR), Privacy and Electronic

6) Identification of privacy solutions

Explain how you could address each risk. Some might be eliminated altogether. Other risks might be reduced. In some cases the chances of risks being realised are small or the impact will be minimal and it may be appropriate to recognise and accept the risks. In these cases the risks should be recorded along with the reasons for accepting the risks.

Evaluate the likely costs and benefits of each approach. Think about the available resources, and the need to deliver a project which is still effective. Consider whether the impact on privacy is proportionate to the aims of the project by balancing the project's outcomes with the impact on individuals. Examples of steps that could be taken to reduce privacy risks include:

- Not collecting or storing some information
- Devising retention periods and planning secure destruction of information
- Using appropriate technology
- Anonymising information when possible
- Producing guidance on the use of the system
- Allowing user access to information so they can correct and access their own data
- Having the necessary agreements in place when data processors are used.
- Having data sharing agreements making it clear what information will be shared and who it will be shared with

For more information about building privacy into a project during the design stages please see the separate

7) Sign off and record of outcomes
Make sure that the privacy risks have been signed-off at an appropriate level. This can be done as part of the wider project approval.

0100090000038d00000002001c000000000040000000301080005000000b020000000050000000c0210055a0e040000002e0118001c000000fb021000070000000000bc020000000001020222537973746 56d0000f08eea1bf08eea1b01000000f08eea1bdc1352ffffffffff040000002d010000040000002d010000040000000201010 01c000000fb02a4ff000000000000900100000000044000224361 6c6962726900000000000000000000000000000000000000000000000000000000000000000040000002d010100040000002d010100040000002d010100050000000902000000020d000000320a570000000100040000000000550e0e052000360005000000090200000002040000002d010000040000002d0100000300000000000

Relevant Legislation

EU General Data Protection Regulations (GDPR)	Regulates the processing of personal data – i.e. information about living identifiable individuals
Article 8 of the Human Rights Act	States that everyone has the right to respect for their private and family life, their home and correspondence. This right is qualified, and exceptions relate to national security, public safety or economic wellbeing of the country, prevention of disorder or crime, protection of health or morals, or of the rights and freedoms of others.
Privacy and Electronic Communications Regulations (PECR)	Regulates electronic direct marketing e.g. email and text messages
Regulatory and Investigatory Powers Act (RIPA)	Regulates the interception of communications data (e.g. phone calls, emails and postal letter), their acquisition and disclosure, the carrying out of covert surveillance etc.
Common law duty of confidence	Points to consider are whether: • the information has the necessary quality of confidence; • the information will be given in circumstances under an obligation of confidence; and • there could be an unauthorised use of the information to the detriment of the confider (although detriment does not always need to exist for a breach of confidence to be actionable) There are four sets of circumstances that make disclosure of confidential information lawful • where the individual to who the information relates has given consent; • where disclosure is in the overriding public interest; • where there is a legal duty to do so, for example a court order; • where there is a statutory basis that permits disclosure.

Appendix 3 – Information required in the event of a Data Protection Breach

Details for the data protection breach

Please describe the incident in as much detail as possible.

a) When did the incident happen?
b) How did the incident happen?
c) If there has been a delay in reporting the incident please explain the reasons for this.
d) What measures were in place to prevent an incident of this nature occurring?
e) Please provide extracts from any policies or procedures considered relevant to this incident, and explain which of these were in existence at the time of this incident. Please provide the dates on which they were implemented.

Personal data placed at risk

f) What personal data has been placed at risk? Please specify if any financial or sensitive personal data has been affected and provide details of the extent.
g) How many individuals have been affected and how many data records are involved?
h) Are the affected individuals aware that the incident has occurred?
i) What are the potential consequences and adverse effects on those individuals?
j) Have any affected individuals complained to the Club about the incident?

Containment and recovery

k) Has any action been taken to minimise/mitigate the effect on the affected individuals? If so, please provide details.
l) Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.
m) What steps have been taken to prevent a recurrence of this incident?

Miscellaneous

n) Have the police or any other regulatory bodies been informed about this incident?
o) Has there been any media coverage of the incident?