

DATA PROTECTION & PRIVACY POLICIES

- The privacy and security of your personal information is extremely important to us. This Data Protection Policy and Privacy Policy explain how and why we use your personal data.
- Dates that individual policies were last reviewed are stated at the end of each section.

Table of Contents

DATA PROTECTION POLICY (MEMBERS)	2
Scope of the Policy.....	2
Why this Policy Exists.....	2
General Guidelines for Committee Members	2
Data Protection Principles	2
Lawful, Fair and Transparent Data Processing	3
Processed for Specified, Explicit and Legitimate Purposes.....	3
Adequate, Relevant and Limited Data Processing	4
Photographs.....	4
Accuracy of Data and Keeping Data Up-to-Date	4
Accountability and Governance.....	4
Secure Processing	4
Subject Access Request.....	5
Data Breach Notification.....	5
PRIVACY POLICY (MEMBERS).....	6
Personal Information Collected	6
How is Personal Information Collected?.....	6
How is Personal Information Used?	6
Who is your Personal Information Shared With?	6
How Long is your Personal Information Kept?	7
How Information can be Updated or Corrected	7
How your Personal Information is Stored	7
Availability and Changes to this Policy	8
Contact.....	8

DATA PROTECTION & PRIVACY POLICIES

DATA PROTECTION POLICY (MEMBERS)

Scope of the Policy

This policy applies to the work of Easingwold Golf Club and sets out the requirements for personal information that Easingwold Golf Club has to gather, store and manage for administration of the activities of the golf club in line with data protection principles and the General Data Protection Regulation. The policy is reviewed on an ongoing basis by the Club to ensure compliance and should be read in tandem with the [Privacy Policy](#) found in a subsequent section of this document.

Why this Policy Exists

This data protection policy ensures Easingwold Golf Club:

- Complies with data protection law and follows good practice
- Protects the rights of members
- Is open about how it stores and processes members data
- Protects itself from the risks of a data breach

General Guidelines for Committee Members

- The only people able to access data covered by this policy should be those who need to communicate with, or provide an administrative or technology assistance service to Easingwold Golf Club members.
- Easingwold Golf Club will, where required, provide training to committee members and others involved with the database system to help them understand their responsibilities when handling data.
- All data shall be kept secure by taking sensible precautions and following the guidelines below.
- Strong passwords should be used and not shared.
- Data should not be shared outside of Easingwold Golf Club unless with prior consent and/or for specific and agreed reasons. Examples would include Gift Aid information provided to HMRC, or information provided to Club Systems Ltd. (who provide and administer the office management system), or BRS Golf (who provide and administer the booking systems).
- Member information should be refreshed periodically to ensure accuracy, via the membership renewal process or when policy is changed.
- Additional support is available from Club Systems Ltd. or BRS Golf where uncertainties or incidents regarding data protection arise.

Data Protection Principles

The General Data Protection Regulation identifies key data protection principles:

- Principle 1: Personal data shall be processed lawfully, fairly and in a transparent manner.
- Principle 2: Personal data must be 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.
- Principle 3: The collection of personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
- Principle 4: Personal data held should be accurate and kept up-to-date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which it is processed, is erased or rectified without delay.

DATA PROTECTION & PRIVACY POLICIES

Principle 5: Personal data must be 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 in so far 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 GDPR in order to safeguard the rights and freedoms of individuals.

Principle 6: Personal data must be 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.

Lawful, Fair and Transparent Data Processing

Easingwold Golf Club requests personal information from potential members and members for membership applications and for sending communications to them about their involvement with Easingwold Golf Club. The forms used to request personal information will contain a privacy statement informing potential members and members as to why the information is being requested and what the information will be used for. The lawful basis for obtaining member information is due to the contractual relationship that Easingwold Golf Club has with individual members. In addition, members will be asked to provide consent for specific processing purposes. Easingwold Golf Club members will be informed as to who they need to contact should they wish their data not to be used for specific purposes for which they have previously provided consent. Where these requests are received they will be acted upon promptly and the member will be informed as to when the action has been taken.

Processed for Specified, Explicit and Legitimate Purposes

Members will be informed as to how their information will be used and the Management Committee of Easingwold Golf Club will seek to ensure that member information is not used inappropriately. Appropriate use of information provided by members will include:

- Communicating with members about their membership application, or renewal of membership;
- Communicating with members about specific issues that may have arisen during the course of their membership;
- Communicating with members about Easingwold Golf Club events and activities including course updates, match information, player participation requests, booking confirmations, handicap information, Management Committee news;
- With prior consent, Club social nights or other functions, Club charity events, donation requests, or offers to Club members;
- With prior consent, communication regarding special offers from local businesses or events at other Clubs;
- Sharing information with various sections of the club, including any disability that you have declared to us, to assist the club in promoting full member inclusion where at all possible;

Easingwold Golf Club will ensure that users are made aware of what would be considered appropriate and inappropriate communication. Inappropriate communication would include sending members marketing and/or promotional materials from external service providers without their prior consent.

Easingwold Golf Club will ensure that members' information is managed in such a way as to not infringe an individual members rights which include:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing

DATA PROTECTION & PRIVACY POLICIES

- The right to data portability
- The right to object

Adequate, Relevant and Limited Data Processing

Members of Easingwold Golf Club will only be asked to provide information that is relevant for membership or charity donation purposes. This will include:

- Title & Name
- Postal address
- Email address
- Telephone numbers
- Handicap Information
- Gift Aid entitlement

Where additional information may be requested such as health related details in accordance with Buggy Policy, or emergency contact details this will only be obtained at the consent of the member, who will be informed as to why this information is required and the purpose that it will be used for. The member themselves must ensure that they have the right to disclose any emergency contact information.

Photographs

Photographs are classified as personal data. Where group photographs are being taken, members will be asked to step out of shot if they do not wish to be in the photograph. Otherwise, consent will be obtained from members in order for photographs to be taken and members will be informed as to where photographs will be displayed. Should a member wish at any time to remove their consent and to have their photograph removed then they should contact the Club Manager to advise that they no longer wish their photograph to be displayed.

Accuracy of Data and Keeping Data Up-to-Date

Easingwold Golf Club has a responsibility to ensure members' information is kept up-to-date. Members will be informed to advise the Club Manager or Administration Assistant if any of their personal information changes. In addition, on an annual basis, the membership renewal process will provide an opportunity for members to inform the Club of any changes to their personal information.

Accountability and Governance

Easingwold Golf Club Management Committee is responsible for ensuring that the Club remains compliant with data protection requirements and can provide evidence to that effect. Where consent is required for specific purposes then evidence of this consent (either electronic or paper) will be obtained and retained securely. Easingwold Golf Club will ensure that new members joining the Management Committee receive an induction into the requirements of GDPR and the implications for their role.

Easingwold Golf Club will also ensure that where data is shared within the Club, outside of the Management Committee members, the necessary responsibilities are understood in relation to any data that may be held or processed. Easingwold Golf Club shall also stay up to date with guidance and practice and shall seek additional input from Club Systems Ltd., BRS Golf, England Golf, or the Information Commissioners Office (ICO) should any uncertainties arise. The Management Committee will review data protection and who has access to information on a regular basis as well as reviewing what data is held. When Committee Members relinquish their roles, they will be asked to either pass on data to those who need it and/or delete data.

Secure Processing

Easingwold Golf Club Management Committee has a responsibility to ensure that data is both securely held and processed. This will include:

DATA PROTECTION & PRIVACY POLICIES

- Restricting access of member information to those on the Management Committee, or those authorised by the Management Committee, who need to communicate with members or administer the system on a regular basis;
- Use of strong passwords;
- Avoidance of password sharing;
- Using password protection on laptops and PCs that contain personal information;
- Using password protection or secure cloud systems when sharing data;
- Ensuring that adequate firewall security is present on all laptops or other devices on which personal data is held.

Subject Access Request

Easingwold Golf Club members are entitled to request access to the information that is held by Easingwold Golf Club. A written request needs to be received by the Club Manager. On receipt, the request will be formally acknowledged and dealt with expediently (the legislation requires that information should generally be provided within one month) unless there are exceptional circumstances as to why the request cannot be granted. Easingwold Golf Club will provide a written response detailing all information held on the member. A record shall be kept of the date of the request and the date of the response.

Data Breach Notification

Should a data breach occur, action shall be taken to minimise the harm. This will include ensuring that all Easingwold Golf Club Management Committee members are made aware that a breach has taken place and how the breach occurred. The Management Committee shall then seek to rectify the cause of the breach as soon as possible to prevent any further breaches. The Club Manager shall contact the Information Commissioners Office within 72 hours of data breach awareness. A discussion will take place between the Club Manager and the Information Commissioners Office as to the seriousness of the breach and action to be taken. The Committee shall also contact, without undue delay, the relevant Club members to inform them of the data breach and actions for resolution.

Where a Club member feels that there has been a breach by Easingwold Golf Club, the Club Manager will ask the member to provide an outline of the breach. If the initial contact is by telephone, the Club Manager will ask the member to follow this up with an email or letter detailing their concern. The alleged breach will then be investigated by members of the Management Committee who are not in any way implicated in the breach. Where the Management Committee or Club Manager needs support, or if the breach is serious, they should notify the Information Commissioners Office. The Club member should also be informed that they can report their concerns to the Information Commissioners Office if they don't feel satisfied with the response from Easingwold Golf Club. Breach matters will be subject to a full investigation, records will be kept, and all those involved notified of the outcome.

[Policy Reviewed: 25th May 2018]

DATA PROTECTION & PRIVACY POLICIES

PRIVACY POLICY (MEMBERS)

Easingwold Golf Club aims to treat your privacy rights seriously. This Privacy Policy sets out how we will deal with your 'personally identifiable information' - that is information that could identify, or is related to the identity of, an individual.

Personal Information Collected

When you express an interest in becoming a member of Easingwold Golf Club you will be asked to provide certain information. This may include:

- title & name;
- home address;
- email address;
- telephone numbers;
- subscription preferences.

We'll only collect the personal data that we need. You may occasionally be asked to be in a photograph that will be posted on the website, included in a newspaper/magazine article, or elsewhere; you can always refuse to give this consent.

How is Personal Information Collected?

All the information collected is obtained directly from you. In order to inform you about the activities and events that you can access we need to store and process a certain amount of personal data. The information will be collected via membership forms, or online contact forms, usually at the point of initial registration. The lawful basis for collecting and storing your information is due to the contractual relationship that you, as a member, will have with Easingwold Golf Club.

You can give us your personal data by completing a paper application form or subsequently, after registration, by providing additional data via our website. We will always ask for your consent to collect and use the data supplied. This may be in the form of an agreement when joining or renewing your membership.

How is Personal Information Used?

We use your personal information:

- To provide our Easingwold Golf Club activities and services to you;
- For the administration, planning and management of Easingwold Golf Club;
- To monitor, develop and improve the provision of our Easingwold Golf Club activities.

Our prime method of message communication to advise you of Easingwold Golf Club activities will be by email, but post, other possible digital methods, or telephone may be utilised as necessary.

Who is your Personal Information Shared With?

We may disclose information about you, including your personal information:

- Internally – to Management Committee members or the Club Professional, as required to facilitate your participation in our Easingwold Golf Club activities;
- Externally – to Club Systems Ltd. for the purposes of providing our management database and resolving any administrative issues, or to BRS Golf for the purposes of providing our tee booking system and resolving any administrative issues;
- Externally – to England Golf for the purposes of running the Central Database of Handicaps (CDH) and for provision of full benefits of membership;
- If we have a statutory duty to disclose it for other legal and regulatory reasons.

DATA PROTECTION & PRIVACY POLICIES

Where we need to share your information outside of the areas stated above we will seek your consent and inform you as to whom the information will be shared and for what purpose.

Easingwold Golf Club members authorised to receive personal information from the database must take reasonable precautions to keep this information secure and confidential. Members must take care not to disclose to unauthorised parties the information, intentionally or otherwise, and must ensure that any information received or gathered is destroyed once the purpose for which it was provided is fulfilled.

How Long is your Personal Information Kept?

We need to keep your information so that we can provide our services to you. In most instances information about your membership will not be stored for longer than a maximum of one year after the member resigns. The exceptions to this are instances where there may be legal or insurance circumstances that require information to be held for longer, whilst the issues are investigated or resolved. Where this is the case, the member(s) will be informed as to how long the information will be held and when it is deleted. Information regarding Gift Aid donations is retained for as long as required under HMRC regulations.

How Information can be Updated or Corrected

To ensure the information we hold is accurate and up-to-date, member's need to inform Easingwold Golf Club as to any changes to their personal information. You can do this by contacting the Club Manager. You can also correct or change any information by logging in to the website (www.easingwoldgolfclub.co.uk) and selecting 'View Personal Details' > 'Change Profile Details' from the viewed web pages. You will also have the opportunity to update your information via the membership renewal process. Should you wish to view the information that Easingwold Golf Club holds regarding yourself, you can make this request by contacting the Club Manager. There may be certain circumstances where we are not able to comply with this request. This would include where the information may contain references to other individuals or for legal, investigative or security reasons. Otherwise we will usually respond within one month of the request being made. No charge will be made for this request.

How your Personal Information is Stored

We have in place a range of security safeguards to protect your personal information against loss or theft, as well as unauthorised access, disclosure, copying, use or modification. Your membership information is primarily held via Club Systems Ltd. on a database (ClubV1) within a cloud based server, security details of which are provided below. Information is integrated with the BRS Golf booking system via the ClubV1 database:

ClubV1 (and all other Club Systems Ltd. cloud software) is hosted in Microsoft Azure's Northern Europe region. Microsoft has been leading the industry in establishing clear security and privacy requirements and consistently meeting these requirements. Microsoft Azure meets a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards, such as Australia IRAP, UK G-Cloud and Singapore MTCS. Rigorous third-party audits, such as by the British Standards Institute, verify Azure's adherence to the strict security controls these standards mandate.

Club Systems Ltd. protects your data in the following ways:

- 1) **Encryption** – Using an industry standard level of Secure Socket Layer (SSL) certification to secure data, the Structured Query Language (SQL) database secures your data by providing encryption for data in motion with Transport Layer Security (TLS) and for data in use with Transparent Data Encryption (TDE);
- 2) **Firewall and Rules** - Firewalls prevent access to the ClubV1 database until specified computers have permission using firewall rules. The firewall grants access to databases based on the originating IP address of each request;
- 3) **Authorisation / Authentication** - Authorisation refers to what a user can do within an Azure SQL Database, and this is controlled by user account permissions. As a best practice, users are granted the least privileges necessary;
- 4) **Dynamic Data Masking** – Some columns are hidden to limit sensitive data exposure by masking them to non-privileged users;

DATA PROTECTION & PRIVACY POLICIES

- 5) **Key Vaults** – Key Vaults are utilised for storing secrets like passwords or Application Programming Interface (API) keys;
- 6) **Additional Security** - All ClubV1 users have an option to use a 'PIN' in conjunction with the Username and Password to ensure an additional level of security, preventing unauthorized access to the Software by any user or other party;
- 7) **Passwords** - Passwords are hashed using unique salts and key stretching to make cracking more difficult.

Along with protection, Club Systems Ltd. also uses proactive monitoring in the form of:

- 1) **Auditing** - Auditing tracks database activities by recording database events to an audit log. Ongoing database activities are able to be understood, as well as analysed and historical activity investigated to identify potential threats or suspected abuse and security violations.
- 2) **Threat Detection** - Threat Detection complements auditing by providing an additional layer of security intelligence built into the service that detects unusual and potentially harmful attempts to access or exploit databases. Club Systems Ltd. is alerted about suspicious activities, potential vulnerabilities and SQL injection attacks, as well as anomalous database access patterns.

Details are only accessed as appropriate by those authorised by the Management Committee to do so. Computers, files and buildings are kept secure. We have received a written assurance declaration from the provider of our database systems that their systems, housing your data, comply with all the security measures required by GDPR.

Availability and Changes to this Policy

This policy is available via the 'Policies' menu link on our website and may change from time to time after review. If we make any material changes we will make members aware via email communication and the Club notice boards.

Contact

If you have any queries about this policy, or have any complaints about our privacy practices, please contact the Club Manager (manager@easingwoldgolfclub.co.uk) of Easingwold Golf Club.

Personal detail updates may be advised to the Club Manager or the Administration Assistant (enquiries@easingwoldgolfclub.co.uk).

[Policy Reviewed: 25th May 2018]