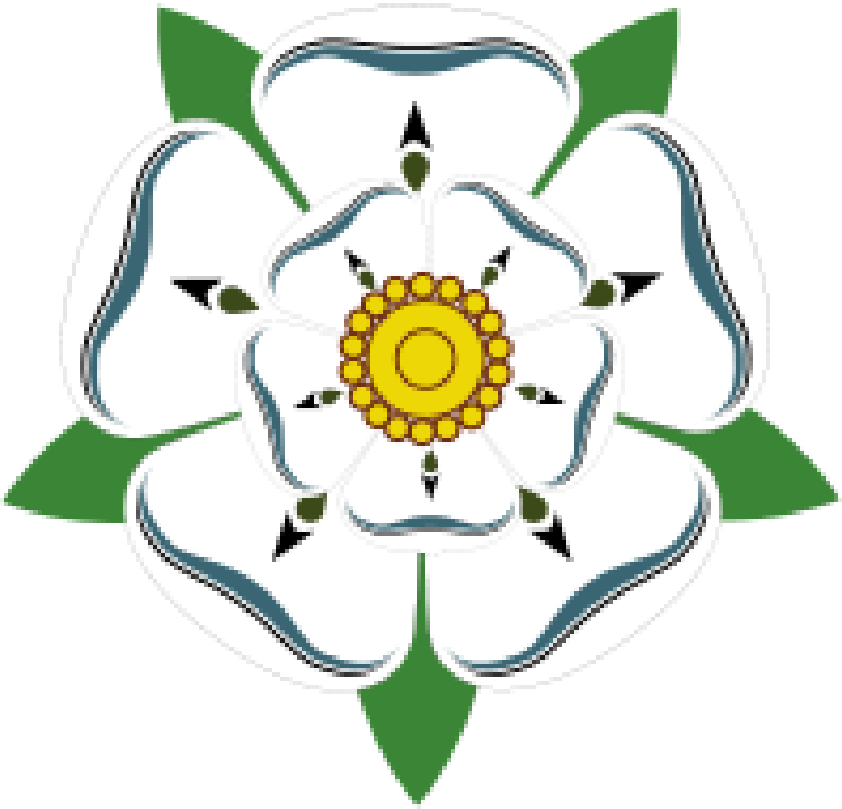
Data Protection, Information Security and GDPR Policy

White Rose Club Ltd



For all members and visitors

Policy Originator	WRCL	Monitoring and Evaluation by	WRCL
Committee Responsible	Current Committee	Date Approved	June 2025
Review Cycle	Annually	Next Review	June 2026
File Reference	WR Data Protection, Information Security and GDPR Policy dated June 2025		

White Rose Club Ltd has a legal duty to comply with the Data Protection Act 2018 which embodies the General Data Protection Regulation (GDPR) and there are substantial fines for non-compliance. This policy sets out the procedures required at White Rose in order to comply. This regulation covers both electronic and paper copies of personal data.

Principles of GDPR:

The UK GDPR sets out seven key principles:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

Good Practice

Good practice requires the Club to:
Know what personal data is held and why it is needed.

1. Carefully consider and be able to justify how long personal data is kept.
2. Regularly review information held and erase personal data when it is no longer needed.
3. Have appropriate processes in place to comply with individuals' requests for erasure under 'the right to be forgotten'.
4. Clearly identify personal data that is needed to be kept in order to meet any statutory requirements.

To achieve this the Club needs to:

1. Document what personal data is held, where it came from and who it is shared with.
2. Be able to show compliance with the data protection principles.
3. Make sure there is a clear opt-in system.

The Club holds personal data for three distinct groups of people.

1. The Club's Members, ex Members and people in the process of becoming Members.
2. Visitors attending the Club for recreational purposes.
3. Tradesmen who have worked or may work on the Club's grounds and Professionals who assist in the running of the Club.

Club Members
Personal data of Club Members, ex Members and people in the process of becoming Members is gathered to allow the effective running of the Club.

Provision of Personal Data to Third Parties
Personal data held by the club must not be divulged to any third party (including other club members) with the following exceptions:

1. Specific data held about those Members who have served or are serving on the Club's Board of Directors as required to be provided to Companies House in accordance with the requirements of the Companies Act 2006.
2. In emergency situations data may be provided to the emergency services as required by them to carry out their statutory duties.

Consent to hold the data and access to it
It is an explicit condition of Club Membership that Members provide specified personal data to be held by the Club. Members have access to the personal data held by the Club on request at any reasonable time and without charge.

Accuracy of data
Members are required to inform the club secretary as soon as possible of any change of personal data. Members will be requested to confirm the accuracy of the data held every year.

Central Computerised record system
Personal data is held on the Club's computer system. The computer is housed in a room with access restricted to current Board Members. The computer hard drive is encrypted. The computer itself is password protected and the data file has its own password. These safeguards must be maintained.

The database may be placed on a "cloud" storage system to assist in the management of the Club. This system must have the same levels of security as the "in office" system.

A secure, encrypted back-up copy of the data file is retained by the club secretary. This is to be used only for recovery purposes in the case of a main system failure.

Website Members Access
Members wishing to access the restricted access areas within the club website need to register. The data provided is used solely to control access to the clubs information and documents provided on the website. Upon discontinuation of membership the Members access is removed and their data is removed in line with the clubs data retention policy.

Other data records held by Directors
Subsets of the data held on the central system are produced to allow specific processes to be carried out effectively. This information may be held electronically (including on Director's personal computers) or on paper. If held electronically it must be held on an encrypted storage medium and password protected. In all the following cases the data must be securely destroyed when the use for which it is provided is completed. The relevant Director is personally responsible for safeguarding the data they hold.

The Company Secretary
Data is held to allow contact with Members to be readily made to enable the Company Secretary to fulfil the post's duties effectively.

The Company Treasurer
Data, including financial data, is held to allow contact with Members to be readily made to enable the Company Treasurer to fulfil the post's duties effectively.

The New Members' Secretary
Data is held to allow the application process to be monitored and contacts be readily made to enable the New Members Secretary to fulfil the post's duties effectively.

Webmaster
Data is held to allow secure access to restricted areas of the club website as appropriate to the status of the individual.

Data records held by non-Directors
From time to time personal data may be provided by a Director to a non-Director for a specific purpose. This data should be restricted to the minimum needed for the specific task, encrypted and password protected and must be securely destroyed after that task has been completed. The Director providing the data is responsible for ensuring compliance in these circumstances.

Retention of data
Personal data of Club Members, ex Members and people in the process of becoming Members will be held on the central computer system for one year after the end of Membership or the application for Membership which does not end in Membership. The Board of Directors may authorise the retention of personal data for longer periods if they deem it necessary as part of a safeguarding policy or to defend the Club's reputation or liabilities.

Provisions for opting out
Whilst it is a condition of Club Membership to provide personal data in order to allow the effective running of the Club any Member may request specific data to be removed from the system in agreement with the club secretary. This may require the Member to make special provisions for contact and the actions to be taken in the case of a sudden loss of membership, a serious accident or death of the Member.

Holiday Visitors
Personal data of visitors attending the Club for recreational purposes is held by the Club to:

1. Control the bookings process.
2. Restricted access to visitor areas of the website.
3. Have a record of the people visiting the Club as part of the safeguarding policy.
4. Contact the Visitors with promotional material.

Provision of Personal Data to Third Parties
With the exception of an emergency situation the data held must not be given to any third party.
In emergency situations data may be provided to the emergency services as required by them to carry out their statutory duties.

Consent to hold the data and access to it
Visitors have to positively consent to the Club retaining their personal data beyond the end of the current calendar year. The Visitor sees and checks all their personal data held by the Club on each visit. In addition, on request Visitors can access the personal data held by the Club at any reasonable time and without charge.

Computerised Visitor record system
Visitors' personal data will be held on the online bookings system. This system is password protected and data is entered by the visitor. Personal data may only be accessed by the bookings team using password protected access and multi factor authorisation. Minimal data is provided to the duty members using a pdf document only allows access to the names of visitors and the timing of their visit.

Other data records held by Directors
Subsets of the data held on the central system are produced for the Club's Directors to assist in the management and control of the Visitor booking system. The amount of personal data on these reports will be kept to the minimum.

Other data records held by non-Directors
The Board authorises Members who are not Directors to manage the booking system and interface with the Visitors. The Board authorises the webmaster to manage access to the club website. The Board is responsible for ensuring compliance in these circumstances.

The Booking Team
The Members designated as above to manage the booking system have full access to all the data held on the booking systems electronic database. They also manage paper based record systems used in the interaction with Visitors and Duty Members.

Webmaster
Data is held to allow secure access to restricted areas of the club website as appropriate to the status of the individual.

Duty Members
Duty Members manage the Visitors on site. They will be given minimal personal data about the Visitors produced by the Booking Team.

Retention of data
Visitor's personal data is retained in the bookings system to facilitate repeat bookings by the visitor and for safeguarding purposes.

Provisions for opting out
If a Visitor, having previously given permission, subsequently requests the Club to remove their personal data from our system this will be done without charge. However the Board of Directors may authorise the retention of personal data for longer periods if they deem it necessary as part of a safeguarding policy or to defend the Club's reputation or liabilities.

Tradesmen and Professionals
In meeting the Club's legal obligations and running of the Club contact is made with many tradesmen, for example, builders, plumbers and electricians who have worked or may work on the Club's grounds and professionals such as accountants and solicitors. Many of these are individuals rather than companies and so personal data may be collected on these individuals from time to time. There is no specific record system and it is therefore the responsibility of the individual Member to safeguard this data and destroy it as soon as it is no longer required.

Information Security

The following rules must be adhered to when accessing personal data:

1. All computers and electronic devices used to access personal data must be password protected and passwords must not be saved onto that device. Electronic areas used for the storing of personal data must be encrypted. All data access programmes must be logged out on leaving the device.

2. Access to personal data must be in a private space where personal data cannot be seen by unauthorised persons.

3. Paper copies of personal data must be kept in a locked filing cabinet and not left on an open surface. They should be securely destroyed when no longer required.

4. Personal data must not be shared with other club members unless express permission is given. For example, if a club member requests the email address of another member, permission should be sought from the member in question to pass on their details.

Sending emails:
All club emails must be sent BCC so that email addresses are not inadvertently shared. Any breach should be reported to the club secretary.

Training:
All members required to access personal data on behalf of the club will be given a copy of this policy and required to sign to confirm that they have read and understood the policy and agree to adhere to it.

White Rose Club Ltd.
Data Protection, Information Security and GDPR Policy

I, the undersigned, confirm that I have received, read and understood the White Rose Club Policy on Data Protection, Information Security and GDPR dated June 2025 and I agree to adhere to the policy.

Name: Date:

Signature:

This page of the document must be retained by the secretary.