[BRISTOL ST ANDREWS BOWLS CLUB]
CLUB POLICY ON GENERAL DATA PROTECTION REGULATIONS (GDPR)
Reviewed Dec 2023 by Data Processor

Introduction – This policy concerns the personal information (**data**) held by the Club, its security and use.

The policy is written in response to the **GDPR**, in force from 25th May 2018. It defines the people involved, the data collected by the Club, how it is stored and used internally and externally, and members' rights over their data.

The Club uses this data solely for the purposes of the effective running of the Club. It also shares the data with the Gloucestershire Bowls Association (GBA) and Bowls England (BE) for their purposes in administering our sport.

The **Data Controller** for the purposes of the GDPR will be the **Club** through the Management Committee. They will be responsible for the implementation and review of this policy. Given the nature of data held and Club size, the appointment of a **Data Protection Officer** is not seen as required; any concerns relating to data protection should be addressed to the **Club Secretary** who will fulfil this role.

The **Data Processor** will be the **Club Secretary** who will hold the club membership database on their computer. The Secretary will be responsible for the collection of the data, its security, ensuring that permission for the data to be held, used, and shared as described below is given, and updating of club records including deletion where required.

What Data is Collected and Why

We collect all contact and membership details to enable us properly to manage and administer your membership with us, the GBA and BE. These details include your contact details, date of birth, gender, and details of a contact in case of emergency. This information is lawfully required and collected as a standard part of your application to join or re-join our Club.

We also need to collect ethnicity and disability information for the purposes of equal opportunities monitoring because we must promote an environment that is inclusive, fair, and accessible. For this information alone, we need your consent to collect it.

The Club does not collect or hold any other 'sensitive data' such as health issues.

When is the Data Collected and Reviewed?

This data is captured when a member first joins the Club through a Club Membership Application form. The accuracy of the personal information will be reviewed annually when a member renews their membership.

Who Collects and Holds the Data?

The data is collected by the Club Secretary. To ensure the security of the data held, the Club requires that access to their computer is password protected and that any file holding the information is also individually password protected.

Sharing Personal Date outside the Club

Data is shared with the Gloucestershire Bowling Association and with the national governing body, Bowls England, so that they too can properly manage and administer your affiliated membership with them. The data is shared via a national Membership Register, the content of which is controlled at all levels by limited and authorised access.

Neither the Club, nor the GBA, nor Bowls England permits the sharing of personal data held on the Membership Register to any third party whatsoever. Specifically, personal data will not be released to any other organisation for marketing or communication purposes.

Where direct consent is given by a member having an identified responsibility or role within their organisation, specific and limited information may be published by the Club, GBA or BE in annual handbooks or on their websites and other social media for the purposes of effective appropriate communication within the sport. The holders of posts within one or more of these organisations will be required to formally consent to the use of specified personal information in this way, and such consent will be recorded by the relevant organisation.

Member's Rights to their Personal Data

Each individual member has the right and the facility to directly access and manage their personal data held on the Membership Register. No one else other than the Club Data Processor has the facility to add or modify personal data. There will be no charge for such access to data. The data held on a member will be deleted within one month of notice that the member has left or is not re-joining the Club.

Young People's Data

GDPR will set an age for a young person to give their own consent to the collection and storage of their personal data. However, given the BE requirements concerning young people, if any club member is below 18, permission for the collection and use of their data will be sought from the parents/guardians of the young person. **Only the name of a young person will be given in the club handbook.** Any member requiring contact with a young person should approach the Secretary to seek agreement for the release of contact details.

Breaches of Data Security

If at any point a breach of data security is suspected or identified, then that suspicion or fact must be reported immediately (verbally if necessary and confirmed in writing) to the Club Secretary who is responsible for investigating breaches of security, determining the resultant degree of risk and deciding on the action to be taken, reporting this at the first opportunity to the Management Committee.

Where a breach is likely to result in a serious risk to the rights and freedoms of individuals (say involving health or financial issues), the Club Secretary has 72 hours to report the incident to the Information Commissioners Office (ICO).

The Club recognises that the requirements of the GDPR apply as much to paper files and records as it does to digital ones and will ensure that any paper records are similarly securely treated. As security issues are much more problematic for paper records, the Club will seek to reduce the use of paper files to the minimum possible. Specifically, membership lists containing personal data will not be displayed on notice boards or the website for public viewing.

Consent on the Holding and Use of the Data

On applying to join the Club, a member will be given a copy of this policy and asked to confirm that they have read and accept it and that the Club may use the personal data in the proper pursuance of managing their relationship with the member.

In addition, members will be asked to consent to the publication of their name and contact details in the Club handbook for communications and so that they and other members can arrange matches as part of Club Competitions.

The Club will use a BCC system when any e-mails are sent to multiple members – to be sent by a club officer only.

Reviews

It is expected that a member will update their personal information if it changes during the year. At the annual subscription, members will be asked to confirm the accuracy of the data held on them. At least every four years, members will be asked to reconfirm their consents as described above.

CCTV Recording and Remote Access

The club being a voluntary organisation and not for profit is exempted from Information Commissioners Office (ICO) registration.

The exemption applies to processing which is only for the purposes of:

- Establishing or maintaining bowls and social membership
- Administering safety control measures activities for either the members or club users
- Accessible if requested by the police

This would include giving support to individuals. It is also clear that although the club Bristol St Andrews has contact with people that should be regular, it does not need to be frequent.

The club provides bowls activities or support on an ongoing basis to the same individuals (even if a minority only contact the organisation once) which falls within exemption.

- Signs are displayed internal and external visible and readable.
- Control who can see the recordings, and make sure the system is only used for the purpose it was intended is via the **Data Controller.**
- To ensure that surveillance camera systems are used only where and when it is necessary
- To ensure an effective administration of the surveillance system
- To ensure that the data is guarded against unauthorised access
- To ensure that the data is disclosed to those who have the legal right to access it
- To retain the data only as long as it is legitimately needed
- To inform surveillance subjects about the use of surveillance equipment, about their rights and about the procedures that they need to follow in order to obtain any data that they are legally entitled to.