Data Protection Policy

Brecon & Radnor Short Mat Bowls Association

Contact email: contactus@brsmba.uk

Contents

1. Overview

1.1 Key details

- Policy prepared by Anthony Morgan, and Vicky Barnett (Data Protection Consultant).
- The Data Protection Contact will be the current Brecon & Radnor Short Mat Bowls Association (BRSMBA) Secretary.
- Approved by Management Committee on 18th May 2025

1.2 Introduction

BRSMBA needs to gather, store and use information about short mat bowls clubs and individual members of the Brecon and Radnor area. This is in order to support the functioning of BRSMBA. It is also to communicate news, event information and details of club and BRSMBA activities.
This policy explains how this data is collected, stored and used including compliance with the UK General Data Protection Regulations (GDPR).
There are also related procedures at the end of the document.

1.4 Why is this policy important?

This policy and related procedures ensure that:

- BRSMBA protects the rights of management committee and the members involved.
- BRSMBA complies with data protection law and follows good practice.
- BRSMBA reduces the risks of a data breach.

2. Roles and responsibilities

2.1 Who and what does this policy apply to?

This applies to the management committee handling data on behalf of BRSMBA.
It applies to all data that the BRSMBA holds relating to individuals, including:

- Names
- Email addresses
- Postal addresses
- Phone numbers
- Shirt Size (if the individual is representing the county in a competition)

2.2 BRSMBA roles and responsibilities

BRSMBA is the data controller and determines what data is collected and how it is used. The Data Protection contact for the BRSMBA is the current serving Secretary. The Secretary along with the other management committee members is responsible for the secure, fair and transparent collection and use of data by BRSMBA. Any questions relating to the collection or use of data should be directed to the Data Protection contact by e-mail to contactus@brsmba.uk.
Everyone who has access to data as part of BRSMBA has a responsibility to ensure that they adhere to this policy and relevant procedures.
BRSMBA ensures as much as possible that all 3rd party data processors are compliant with GDPR.

3. Data protection principles

a. **We fairly and lawfully process personal data in a transparent way.**

b. **We only collect and use personal data for specific, explicit and legitimate purposes and will only use the data for those specified purposes.**

There is a BRSMBA privacy statement available on the Information Page of the BRSMBA website along with a list of the current serving management committee members: - https://brsmba.uk/information/.

BRSMBA only collects data where lawful and where it is necessary for the legitimate purposes of the group.

- The management committee members contact details are collected when they first join the committee and are used to contact them regarding the ongoing administration of the BRSMBA and activities relating to their roles. The basis for this is legitimate interest as when a person joins the committee it is reasonably expected that they may receive such information.

- The name and contact details of BRSMBA member are collected when they join and updated annually; and are used to contact them regarding BRSMBA administration and activities. The basis for this is legitimate interest as when a person (re)joins the BRSMBA it is reasonably expected that they may receive such information.

- Consent forms / e-mails are kept as evidence of consent as long as this is needed. The basis of this is legal obligation.

c. We ensure any data collected is relevant and not excessive

BRSMBA does not collect or store more data than the minimum information required for its intended purpose.

d. We ensure data is accurate and up-to-date

BRSMBA does a check every two years on the database to determine if there is any obviously inaccurate data.

When items are returned saying that a person no longer lives at that address or e-mail addresses or phone numbers are no longer valid this information is corrected including deletion where necessary.

e. We keep personal data secure

BRSMBA ensures that data held is kept secure.

- Stored physically and electronically in the homes of management committee members who need access to this.
- Access to data is only given to relevant management committee members where it is clearly necessary for the running of the BRSMBA.
- E-mails and e-mail lists are stored on e-mail provider servers such as Gmail.
- Mobile numbers are stored by the WhatsApp server.

4. Individual Rights

When the BRSMBA collects, holds and uses an individual's personal data that individual has the following rights over that data. The BRSMBA ensures its data processes comply with those rights and makes all reasonable efforts to fulfil requests from an individual in relation to those rights.

4.1 Individual's rights

Right to be informed: There is a BRSMBA privacy notice which is given to individuals when their data is taken. This may be given on paper or electronically including an electronic link.

Right of access: Individuals can request to see the data BRSMBA holds on them and confirmation of how it is being used. Requests should be made in writing to the Data Protection contact and are complied with free of charge and within one month.

Right to rectification: Individuals can request that their data be updated where it is inaccurate or incomplete. Any requests for data to be updated are processed within one month.

Right to object: Individuals can object to their data being used for a particular purpose. The BRSMBA provides ways for an individual to withdraw consent in all marketing communications. Where there is a request received to stop using data the BRSMBA complies unless there is a legal, contractual or legitimate interest reason to use the data.

Right to erasure: Individuals can request for all data held on them to be deleted. This is carried out unless there is a legal, contractual or legitimate interest reason to keep the data.

5. How we get consent

Individuals can request to join the BRSMBA WhatsApp group at any time; they will be sent a WhatsApp invitation, which they can then choose to "Accept" or "Reject".
The BRSMBA will also collect data annually from the secretaries of each of the short mat bowls clubs that are part of the BRSMBA. This data will provide a method for users to show their positive and active consent to continue to be a part of the BRSMBA WhatsApp group (e.g. a 'tick box').

All the collected data will then be reviewed by the Data Protection contact and amended as necessary.

Data collected will only ever be used in the way described and consented to (e.g. we will not use data in order to market 3rd-party products unless this has been explicitly consented to).

Individuals can withdraw from the WhatsApp group at any time by sending an email to the Data Protection contact (brshortmat@gmail.com) ; requesting that they are removed from the WhatsApp group. Opt-out requests such as this are processed within one month.

6. Data retention policy and Procedures

6.1 Overview

6.1.1 Introduction

This policy sets out how the BRSMBA approaches data retention and establishes processes to ensure data is not held for longer than is necessary.

6.1.2 Roles and responsibilities

BRSMBA is the data controller and determines what data is collected, retained and how it is used. The Data Protection contact for the BRSMBA is the current Secretary. They, together with the BRSMBA committee members are responsible for the secure and fair retention and

use of data by BRSMBA. Any questions relating to data retention or use of data should be directed to the Data Protection contact.

6.2 Regular Data Review

An annual data audit will be carried out and documented to determine the description of data, why it is held, what it is used for, the basis for processing, who holds the data, who can access it, what security controls are in place, how long data is kept for, is it covered by the policy and privacy notice and recommended actions. Further data audits are carried out and documented on significant changes. If necessary a consultant can assist with this process.

In addition to the audits a regular review of all data takes place to establish if the BRSMBA still has good reason to keep and use the data held at the time of the review. As a general rule a data review is held every 2 years and no more than 27 calendar months after the last review. Records are taken as evidence of this review.

6.2.1 Data reviewed

- Mobile contact numbers held locally by committee members.
- Databases.
- Data stored on third party online services such as Gmail Contacts
- Paper forms.
- Consent evidence.

6.2.2 Who the review is conducted by

The review is conducted by the Data Protection contact with other committee members to be decided on at the time of the review. If necessary a consultant can assist with this process.

6.2.3 How data will be deleted

All reasonable and practical efforts are made to remove data stored digitally including backups.

6.2.4 Criteria

The following criteria will be used to make a decision about what data to keep and what to delete. Evidence is kept of the answers to the questions and the actions taken.

Question	Action	
	Yes	**No**
Is the data stored securely?	No action necessary	Update storage arrangements in line with policy
Does the original reason for having the data still apply?	Continue to use	Delete or remove data
Is the data being used for its original intention?	Continue to use	Either delete/remove or record lawful basis for use and get consent if necessary
Is there a statutory requirement to keep the data?	Keep the data at least until the statutory minimum no longer applies	Delete or remove the data unless we have reason to keep the data under other criteria
Is the data accurate?	Continue to use	Delete or remove incorrect data. Ask the subject for updated details if they have changed
Where appropriate do we have consent to use the data with evidence of consent?	Continue to use	Get consent
Can the data be anonymised?	Anonymise data	Continue to use
Is there any data not covered in the policy, notice and procedures?	Carry out audit of this data and update notices, policy and procedures where needed.	No action.

6.2.4 Statutory Requirements

Data stored by the BRSMBA may be retained based on statutory requirements for storing data other than data protection regulations. This might include but is not limited to:

- Details of payments made and received (e.g. in bank statements and accounting records).
- Committee meeting minutes.
- Contracts and agreements with suppliers/customers.
- Insurance details.

6.3 Other Data Retention Procedures

6.3.1 Committee data

- When a committee member of the BRSMBA leaves and all administrative tasks relating to their involvement have been completed, any potentially sensitive data held on them must be deleted.
- Unless consent has been given data must be removed from all email mailing lists.
- All other data must be stored safely and securely and reviewed as part of the next data review.

6.3.2 WhatsApp group list data

- If an individual chooses to opt out of the WhatsApp group their data must be removed from the WhatsApp contacts as soon as is practically possible within the one month legal requirement.
- All other data must be stored safely and securely and reviewed as part of the annual data review.

6.3.4 Other data

- All other data must be included in a regular data review.

7. Data Rights Requests

7.1 Procedure

If a request is received from a data subject that relates or could relate to their data protection rights, this must be forwarded to the Data Protection contact immediately. The Data Protection contact is the current BRSMBA Secretary.
This could include the following request by the data subject:

a. request access to any of their personal data held (known as a Subject Access Request - SAR);
b. ask to have inaccurate personal data changed;
c. ask to have data deleted;
d. withdraw consent when consent is relied upon to process their data.

Requests may be verbal or written. However, if a verbal request is received a written request should be asked for if possible. If no written request is forthcoming the request must be documented by the Data Protection contact or someone who they nominate.

Valid requests must be acted upon as soon as possible, and at the latest within one calendar month, unless the timescale can lawfully extend up to two months (in some circumstances).

All data subjects' rights request actions must be provided free of charge.

Any information provided to data subjects must be documented in a concise and transparent way, using clear and plain language.

Records of all requests and responses must be maintained by the data protection contact.

8. Data Protection Breach

8.1 Procedure

Where committee members think that the data protection policy has not been followed, or data might have been breached or lost, this must be reported immediately to the Data Protection contact.

Records of personal data breaches must be kept by the Data Protection contact even if they are not reported to the Information Commissioners Office (ICO).

Data breaches which are likely to result in a risk to any person must be reported to the ICO. Reports must be made to the ICO within 72 hours from when someone on the steering committee becomes aware of the breach.

In situations where a personal data breach causes a high risk to any person. As well as reporting the breach to the ICO, the data subjects must be informed without undue delay. Informing data subjects can enable them to take steps to protect themselves and/or to exercise their rights.

The ICO's address:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
Helpline number: 0303 123 1113
ICO website: https://www.ico.org.uk

It should be noted that data breaches may also be reported directly to the ICO by the person who has identified a breach and as such first contact may come from the ICO.

9. Change of Data Processing

9.1 Procedure

If additional data is to be processed a data audit must be carried out for this data and where necessary policy and procedures changed. Any changes must be communicated to relevant parties.

10. IT Security Policy

10.1 Procedure

If computers, laptops, mobile phones or tablets are being used in the BRSMBA related personal data processing including storage the following must be carried out:

- Set and use a passcode (e.g. pin number or password) to access your device.
- Set your device to lock automatically when it is inactive for more than a few minutes.
- The above two do not need to be carried out for a desktop that is permanently kept in a secure home or office and where the personal data is encrypted/password protected.
- Be security conscious to ensure your device cannot easily be stolen. Do not leave it unattended or in open view in a locked car.
- Back up your documents securely.
- Keep your software up to date including security updates.
- Report any data breaches in accordance with the policy.
- Exercise caution when opening files attached to emails.
- Use anti-virus software and keep it up to date.
- Be careful about connecting to unsecured wireless networks.
- Disable services such as Bluetooth and wireless if you are not using them
- Store data in databases and files locally and on a secure cloud.

In addition for mobile phones and tablets:

- Configure your device to enable you to remote-wipe should it become lost.
- If your device is second hand, restore to factory settings before using it for the first time.
- Only download applications (‘apps’) or other software from reputable sources.

11. Review of Policies and Procedures

All BRSMBA Policies and Procedures will be reviewed on a regular basis (< 12 months) and recorded in the Policies and Procedure log.

A summary of any changes made to this document will also be recorded in the Policies and Procedure Log.