RESIDENTS' ASSOCIATION OF WEST WIMBLEDON ("RAWW")

Data Protection Policy

SCOPE OF THE POLICY

This policy applies to the work of RAWW. The policy sets out the requirements that RAWW has to gather personal information for membership purposes. The policy details how personal information will be gathered, stored and managed in line with data protection principles and the General Data Protection Regulation. The policy is reviewed on an ongoing basis by the RAWW committee members to ensure that RAWW is compliant. This policy should be read in tandem with RAWW's Privacy Policy.

WHY THIS POLICY EXISTS

This data protection policy ensures that RAWW:

- 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 a service to the members of RAWW.
- Data should not be shared informally or outside of RAWW.
- Committee Members should keep all data secure, by taking sensible precautions and following the guidelines below.
- Strong passwords must be used and they should never be shared.
- Personal data should not be shared outside of RAWW unless with prior consent of the member concerned.
- Member information should be reviewed periodically via the membership renewal process.
- Committee members should confer with the Treasurer of RAWW if they are unsure about any aspect of data protection.

DATA PROTECTION PRINCIPLES

The General Data Protection Regulation identifies 8 data protection principles.

Principle 1 - Personal data shall be processed lawfully, fairly and in a transparent manner

Principle 2 - Personal data can only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Principle 3 - The collection of personal data must be adequate, relevant and limited to what is necessary compared to the purpose(s) data is collected for.

Principle 4 – Personal data held should be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.
Principle 5 – Personal data which is kept in a form which permits identification of individuals shall not be kept for longer than is necessary.
Principle 6 - Personal data must be processed in accordance with the individuals' rights.
Principle 7 - 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.
Principle 8 - Personal data cannot be transferred to a country or territory outside the European Union unless that country or territory ensures an adequate level of protection for the rights and freedoms of individuals in relation to the processing of personal data.

Lawful, fair and transparent data processing
RAWW requests personal information from potential members and members for the purpose of sending communications about the activities of RAWW. 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 privacy notice will inform potential members and members that the legal basis for processing and holding their personal data is because RAWW has a legitimate interest in that data - this means that RAWW's processing is necessary for the purposes of the legitimate interests pursued by RAWW except where such interests are overridden by the interests or fundamental rights and freedoms of the potential member or member which require protection of personal data. RAWW members will be informed that they can, at any time, request that their personal data be erased. Once a member requests that their data be erased this 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 RAWW Committee will seek to ensure that member information is not used inappropriately. Appropriate use of information provided by members will include:

- Communicating with members about RAWW's work and activities
- Communicating with members about specific issues that may have arisen during the course of their membership and which are likely to be of interest to persons living in West Wimbledon and adjacent areas.
- Communicating with members about their membership and/or renewal of their membership.

RAWW 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.
- The right to data portability.
- The right to object.

Adequate, Relevant and Limited Data Processing
Members of RAWW will only be asked to provide information that is relevant for membership purposes. This will include:

- Name
- Postal address
- Email address
- Telephone number
- Age range (optional)

Where additional information may be required this will be obtained with the specific consent of the member who will be informed as to why this information is required and the purpose that it will be used for.

Accuracy of Data and Keeping Data up to Date
RAWW has a responsibility to ensure members' information is kept up to date. Members will be requested to let the membership secretary know if any of their personal information changes. In addition, on an annual basis the membership renewal forms will provide an opportunity for members to resubmit their personal information.

Accountability and Governance
The RAWW Committee are responsible for ensuring that RAWW remains compliant with data protection requirements and can evidence that it has. The Committee will carry out and document a Legitimate Interests Assessment each year. The RAWW Committee shall ensure that new members joining the Committee receive an induction into how data protection is managed within RAWW and the reasons for this. The Committee will review data protection and who has access to information on an annual basis as well as reviewing what data is held.

Secure Processing
The RAWW committee members have a responsibility to ensure that data is both securely held and processed. This will include:

- Committee members using strong passwords on spreadsheets containing membership data.
- Committee members not sharing passwords.
- Restricting the sharing member information to those on the Committee who need to communicate with members on a regular basis and the Treasurer of RAWW.
- Using password protection on laptops and PCs that contain or access personal information.
- Using password protection or secure cloud systems when sharing data between committee members.

- Those Committee Members' laptops and PCs that hold personal data having up-to-date firewall and anti-virus software.

RAWW will use MailChimp, a USA based online email marketing platform, to send communications to members. The only personal data that will be stored on MailChimp is the name and email address of the member. MailChimp states that it is compliant with the EU-US Privacy Shield programme and RAWW has entered into a Data Processing Agreement with MailChimp dated 18 May 2018.

Subject Access Request

A RAWW member is entitled to request access to the information that is held on him/her by RAWW. The request needs to be received in the form of a written request to the Membership Secretary of RAWW. On receipt of the request, the request will be formally acknowledged and dealt with within 14 days unless there are exceptional circumstances as to why the request cannot be granted. RAWW 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

Were a data breach to occur action shall be taken to minimise the harm by ensuring all committee members are aware that a breach had taken place and how the breach had occurred. The committee shall then seek to rectify the cause of the breach as soon as possible to prevent any further breaches. The Chair and the Treasurer shall consider the seriousness of the breach, the action to be taken and, where necessary, the Information Commissioner's Office would be notified. The committee shall also contact the relevant members to inform them of the data breach and actions taken to resolve the breach.

If a RAWW member contacts RAWW to say that they feel that there has been a data breach by RAWW, a committee member will ask the member to provide an outline of their concerns. If the initial contact is by telephone, the committee member will ask the member to follow this up with an email or a letter detailing their concern. The concern will then be investigated by members of the committee who are not in any way implicated in the breach. Breach matters will be subject to a full investigation, records will be kept and all those involved notified of the outcome.

Policy review date: August 2020