WDPS Data Protection Policy

Scope of the policy

This policy applies to the activities of Wheathampstead and District Preservation Society ("WDPS"). The policy sets out the requirements that WDPS has to gather 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 WDPS committee members to ensure that we are compliant. This policy should be read in tandem with WDPS's Privacy Policy.

Why this policy exists

This data protection policy ensures WDPS:

- 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 WDPS members.
- 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 except where password protected files are shared.
- Data should not be shared outside of WDPS unless with prior consent and/or for specific and agreed reasons.
- Member information should be refreshed periodically to ensure accuracy.

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 they are processed;

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, having regard to the purposes for which they are processed, are erased or rectified without delay;

Principle 5 – Personal data must kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for the which the personal data are processed; personal data may be stored for longer periods insofar 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 accordance 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

WDPS requests personal information from potential members and members for membership applications and for sending communications about their involvement with WDPS. 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 WDPS has with individual members. WDPS members will be informed as to who they need to contact should they wish for their data not to be used for specific purposes for which they have 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 Committee of WDPS will seek to ensure that member information is not used inappropriately. Appropriate use of information provided by members will include:

- Communicating with members about WDPS events and activities
- Communicating with members about local activities that may be of interest and in line with WDPS objectives
- Communicating with members about their membership and/or renewal of their membership
- Communicating with members about specific issues that may have arisen during the course of their membership

WDPS will ensure that committee members are made aware of what would be considered appropriate and inappropriate communication.

WDPS 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 WDPS will only be asked to provide information that is relevant for membership purposes. This will include:

- Name
- Postal address
- Email address
- Telephone number
- Subscription preferences

Photographs

Photographs are classified as personal data. Where group photographs are being taken members will be asked to step out of shot if they don't wish to be in the photograph. Should a member wish at any time to remove their consent and to have their photograph removed then they should contact **info@wheathampsteadpreservation.org.uk** to advise that they no longer wish their photograph to be displayed.

Accuracy of data and keeping data up-to-date

WDPS has a responsibility to ensure members' information is kept up to date. Members will be informed to let the membership secretary know if any of their personal information changes.

Accountability and governance

The WDPS Committee are responsible for ensuring that WDPS remains compliant with data protection requirements and can evidence that it has done so. Where consent is required for specific purposes then evidence of this consent (either electronic or paper) will be obtained and retained securely. The WDPS Committee will ensure that new members joining the Committee are aware of this policy and the requirements of GDPR and the implications for their role.

Secure Processing

WDPS Committee Members have a responsibility to ensure that data is both securely held and processed. This will include:

- Committee members using strong passwords
- Committee members not sharing passwords, other than when sharing password protected files
- Restricting access of sharing member information to those on the Committee who need to communicate with members on a regular basis
- Using password protection on laptops and PCs that contain personal information
- Using password protection or secure cloud systems when sharing data between committee members

Subject Access Request

WDPS members are entitled to request access to the information that is held by WDPS. The request needs to be received in the form of a written request to the Membership Secretary of

WDPS. On receipt of the request, the request will be formally acknowledged and dealt with expediently and within one month unless there are exceptional circumstances as to why the request cannot be granted. WDPS 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

If a data breach were to occur, action will be taken to minimise the harm. This will include ensuring that all WDPS Committee Members are made aware that a breach has taken place and how the breach occurred. The Committee will then seek to rectify the cause of the breach as soon as possible to prevent any further breaches. The Chair of WDPS will decide whether the Information Commissioner's Office should be notified. The Committee will also contact the relevant WDPS members to inform them of the data breach and actions taken to resolve the breach.

Where a WDPS member feels that there has been a breach by WDPS, a committee member will ask the member to provide an outline of the breach. If the initial contact is by telephone, the committee member will ask the WDPS member to follow this up with an email or a letter detailing their concern. The alleged breach 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 will be notified of the outcome.