Chilton Polden Hall Data Protection Policy

Scope of the policy

This policy applies to the work of Chilton Polden Hall. The policy sets out the need to gather information and 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 Committee Members to ensure that we are compliant. This policy should be read in tandem with Chilton Polden Hall's Privacy Policy.

Why this policy exists

This data protection policy ensures Chilton Polden Hall:

- Complies with data protection law and follows good practice
- Protects the rights of users
- Is open about how it stores and processes 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 Chilton Polden Hall users.
- 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.
- Data should not be shared outside of the Committee unless with prior consent and/or for specific and agreed reasons.

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 it is 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 inaccurate personal data, having regard to the purposes for which they are processed, is erased or rectified without delay

Principle 5 – Personal data must be 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 is 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 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

Chilton Polden Hall Committee requests personal information from potential users and for sending communications about their involvement with Chilton Polden Hall.

Data processing for specified, explicit and legitimate purposes

Individuals will be informed as to how their information will be used and the Committee will seek to ensure that personal information is not used inappropriately. Appropriate use of information provided by members will include communicating with Chilton Polden Hall users.

Chilton Polden Hall Committee will ensure that individual's information is managed in such a way as to not infringe the individual's 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

Users will only be asked to provide information that is relevant. This will include:

- Name
- Telephone number
- Email address

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

Photographs

Photographs are classified as personal data. However, GDPR does not apply to photographs taken in a public place. Elsewhere, 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. Otherwise consent will be obtained in order for photographs to be taken and people will be informed as to where photographs will be displayed. Should an individual wish at any time to remove their consent and to have their photograph removed then they should contact the Secretary by email to advise that they no longer wish their photograph to be displayed.

Accuracy of data and keeping data up-to-date

Chilton Polden Hall has a responsibility to ensure individuals' information is kept up to date. Individuals should let the Secretary know if any of their personal information changes.

Accountability and governance

The Chilton Polden Hall Committee are responsible for ensuring that Chilton Polden Hall 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 Chilton Polden Hall Committee will ensure that new members joining the Committee receive an induction into the requirements of GDPR and the implications for their role. The Committee will review data protection and who has access to information on a regular basis as well as reviewing what data is held. When Committee Members relinquish their roles, they will be asked to either pass on data to those who need it and/or delete data.

Secure processing

Chilton Polden Hall 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
- Restricting access of sharing information to those on the Committee who need to communicate with users 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.
- Paying for firewall security to be put onto Committee Members' laptops or other devices.

Subject access request

Individuals are entitled to request access to the information relating to them that is held by Chilton Polden Hall. The request needs to be received in the form of a written request to the Secretary. On receipt of the request, the request will be formally acknowledged and dealt with expediently (the legislation requires that information should generally be provided within one month) unless there are exceptional circumstances as to why the request cannot be granted. Chilton Polden Hall 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. This will include ensuring that all Chilton Polden Hall Committee Members are made aware that a breach has taken place and how the breach occurred. The Committee shall then seek to rectify the cause of the breach as soon as possible to prevent any further breaches. The Committee shall also contact the relevant individuals to inform them of the data breach and actions taken to resolve the breach.

Where an individual feels that there has been a breach by Chilton Polden Hall, a Committee Member will ask the individual to provide an outline of the breach. If the initial contact is by telephone, the Committee Member will ask the individual to follow this up with an email or 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 notified of the outcome.

Last reviewed: June 2018