HCACR Data Protection Policy

(Last updated 18/2/25)

## Scope

This policy applies to the work of the Hertford County Association of Change ringers (hereafter ‘HCACR’). The policy sets out the requirements that the HCACR 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 HCACR general management committee members (hereafter GMC) to ensure that the HCACR is compliant. This policy should be read in tandem with the HCACR's Privacy Policy.

# Why this policy exists

This data protection policy ensures that the HCACR:

* Complies with data protection law and follows good practice.
* Protects the rights of members, officers and committee 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 the HCACR.
* Data should not be shared informally or outside of the HCACR, save for the purposes of membership management and production of the Annual Report.
* Committee Members should keep all data secure, by taking sensible precautions and following the guidelines below.
* Strong passwords must be used and should never be shared.
* Personal data should not be shared outside of the HCACR unless with prior consent and/or for specific and agreed reasons.
* Member information should be reviewed and consent refreshed periodically via the membership renewal process.

## Data processing

The HCACR requests personal information from members and potential members for the running of the HCACR. The HCACR uses a third-party membership management system. The system and on-line form used to request personal information refers to a privacy statement informing members and potential members as to why the information is being requested and what the information will be used for. Members will be asked to consent for their data to be held and a record of this consent along with member information will be securely held. HCACR members will be informed that they can, at any time, remove their consent and will be informed as to who to contact should they wish to do so. Once an HCACR member requests their data to be removed this will be acted upon promptly and the member will be informed when this has been actioned.

## Processed for Specified, Explicit and Legitimate Purposes

Members will be informed as to how their information will be used and the Committee of the HCACR will seek to ensure that member information is not used inappropriately. Appropriate use of information provided by members will include:

* Maintaining a membership database.
* Communicating with members about the HCACR’s events and activities
* Publicising HCACR activities in the Ringing World and on social media.
* Sending members information about bell ringing events and activities.
* 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.
* Providing other bell ringers and bell ringing associations with information to further the ideals of bell ringing.
* When claiming gift aid.

The HCACR will ensure that association officers are made aware of what would be considered appropriate and inappropriate communication. Inappropriate communication would include sending HCACR members marketing and/or promotional materials from external service providers not associated with bell ringing.

The HCACR will ensure that members' information is managed in such a way as to not infringe their rights

## Adequate, Relevant and Limited Data Processing

Members of the HCACR will only be asked to provide information that is relevant for membership purposes. This will include:

* Name.
* Postal address.
* Email address.
* Telephone number.

If any additional information is required, such as health-related information, 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.

There may be occasional instances where a members' data needs to be shared with a third party due to an accident or incident involving statutory authorities. Where it is in the best interests of the member or the HCACR, in these instances where the HCACR has a substantiated concern, then consent does not have to be sought from the member.

## Accuracy of Data and Keeping Data up to Date

The HCACR has a responsibility to ensure members' information is kept up to date. Members can manage and update their information at any time through the membership management system. Alternatively, they can let their district secretary know if any of their personal information changes.

## Accountability and Governance

The HCACR GMC are responsible for ensuring that the HCACR remains compliant with data protection requirements and can evidence that it has. For this purpose, those from whom data is required will be asked to provide written consent. This will then be securely held as evidence of compliance. The HCACR GMC shall ensure that new members joining the Committee receive an induction into how data protection is managed within the HCACR and the reasons for this. GMC Members shall also stay up to date with guidance and practice within the bell ringing movement and shall seek additional input from the CCCBR should any uncertainties arise. The GMC will review data protection and who has access to information on a regular basis as well as reviewing what data is held.

## Secure Processing

The GMC members of the HCACR have a responsibility to ensure that data is both securely held and processed. This will include:

* Using a membership management system which is GDPR compliant.
* Using strong passwords.
* Not sharing passwords.
* Restricting access of 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 or access personal information.
* Using password protection or secure cloud systems when sharing data between committee members.
* Ensuring Committee Members' laptops or other devices have firewall security on them.

## Subject Access Request

HCACR members are entitled to request access to the information that is held by the HCACR. This needs to be received in writing by their District Secretary. On receipt of the request, this will be formally acknowledged and dealt with within 21 days unless there are exceptional circumstances as to why the request cannot be granted. The HCACR 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 Secretary of the HCACR shall contact all committee members within 48 hours of the breach occurring to notify of the breach. A discussion would take place between the Secretary and committee as to the seriousness of the breach, action to be taken and, where necessary, the Information Commissioner's Office would be notified. The committee shall also contact the relevant HCACR members to inform them of the data breach and actions taken to resolve the breach.

If an HCACR member contacts the HCACR to say that they feel that there has been a breach by the HCACR, 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 HCACR 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.