Aylesbury Choral Society

Chairman: Dr Christopher Dalladay
acschairman@gmail.com

website: www.aylesburychoral.org.uk

Data protection and retention

June 2025

Policy prepared by:	Dr Christopher Dalladay (Chair, ACS)
Approved by committee on:	July 2025
Next Review date:	1st September 2027

Introduction

In order to operate, The Aylesbury Choral Society ("the Society" or "ACS") needs to gather, store and use certain forms of information about individuals. These individuals can include members, volunteers, staff, freelancers, contractors, audiences and potential audiences, business contacts and other people the Society has a relationship with or regularly needs to contact. This range of individuals will be referred to as "the individuals" throughout this policy document.

This policy explains how this data should be collected, stored and used in order to meet ACS data protection standards and comply with the General Data Protection Regulations (GDPR). It has been written under guidance from *Making Music* (The National Federation of Music Societies), of which ACS is a member.

Why is this policy important?

This policy ensures that ACS:

- Protects the rights of our members, volunteers and supporters, and all individuals associated with it.
- Complies with data protection law and follows good protection.
- Protects the members of the Society and other individuals from the risks of a data breach.

This applies to *all* those handling data on behalf of ACS, e.g.:

- Committee members
- Staff and volunteers
- Members
- Contractors / 3rd party suppliers (e.g. lighting and staging contractors)

It applies to all data that ACS holds relating to individuals, including:

- Names
- Email and postal addresses
- Phone numbers
- Voices and roles within the Society
- Any other personal information held (e.g. financial)

Roles and responsibilities

ACS is the Data Controller and will determine what data is collected and how it is used.
The Data Protection Officer (DPO) for ACS is the chairman or, when the chair is not available, the webmaster. However, membership data (e.g. name and contact details) is also collected by the Membership Secretary and financial data (e.g. details of 'subs' paid) by the Society's Treasurer. The DPO together with Society's committee are responsible for the secure, fair and transparent collection and use of data by ACS. Any questions relating to this should be directed to the DPO.

Everyone who has access to data as part of ACS has a responsibility to ensure that they adhere to this policy.

ACS uses third party Data Processors (e.g. *Making Music Platform*) to process data on its behalf. ACS will ensure that all Data Processors are compliant with GDPR.

Data Protection principles

(1) We fairly and lawfully process personal data in a transparent way.

- A member's name and contact details will be collected when they first join ACS, and will be used to contact the member on matters regarding group membership, administration and activities. Other data may also be collected in relation to their membership, including their payment history for 'subs' and other financial dealings in reasonable functions of the Society.
- The name and contact details of other individuals when they take up a position or contribute to the functioning of the Society (e.g. lighting contractors), and they will be used to contact them regarding group administration related to their role.
- Further information, including personal financial information (e.g. bank details), may also be collected in specific circumstances where lawful and necessary (e.g. in order to carry out bank transfers in payment for services).
- An individual's name and contact details *may* be collected when they make a booking for an event (e.g. in the purchase of concert tickets). This will be used to contact them about their booking and to allow them entry to the event.
- An individual's name and contact details and other details *may* be collected at any time (e.g. for upkeeping mailing lists), with their consent, in order for ACS to communicate with them about and promote group activities.
- Pseudonymous or anonymous data on an individual may be collected through the use of Cookies when using the Society's website or interacting with our emails. See the section below on 'Cookies' for further information regarding these.

(2) We only collect and use personal data for specific, explicit and legitimate purposes and will only use the data for those specified purposes.

- When collecting data, ACS will always provide a clear and specific privacy statement explaining to the subject why the data is required and what it will be used for.

(3) We ensure any data collected is relevant and not excessive.

- ACS will not collect or store more data than the minimum information required for its intended purpose.

(4) We ensure data is accurate and up-to-date

- ACS will ask members, volunteers and staff to check and update their data on an annual basis. Members will have a personal and private access their own personal data held on our private administrative system and which is accessible through our website. Any individual will be able to update their data at any point by contacting the DPO or Membership Secretary.

(5) We ensure data is not kept longer than necessary.

- ACS will keep records for no longer than is necessary in order to meet the intended use for which it was gathered (unless there is a legal requirement to keep records).

(6) We keep personal data secure

- Electronically held data will be held within a password protected and secure environment.
- Passwords for electronic data will be reset each time an individual with data access leaves their role/position.
- Physically held data (e.g. membership forms or email sign-up sheets) will be stored in a locked cupboard/cabinet.
- Access to data will only be given to relevant committee members / contractors where it is clearly necessary for the running of the group. The DPO will decide in what situations this is applicable and keep a master list of who has access to data.

(7) Transfer to countries outside the EEA

- ACS will not transfer data to countries outside the European Economic Area (EEA) unless the country has adequate protection for the individual's data privacy rights.

Individual Rights

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

- *Right to be informed:* Whenever ACS collects data it will provide a clear and specific privacy statement explaining why it is being collected and how it will be used.
- *Right of access:* Individuals can request to see the data ACS holds on them and confirmation of how it is used. Requests should be made in writing to the DPO and will be complied with free of charge and within one month. Where requests are complex or numerous this may be extended to two months.
- *Right to rectification:* Individuals can request that their data be updated where it is inaccurate or incomplete. ACS will request that members, staff and contractors check and update their data on an annual basis. Individuals can access their own personal data held on the Society's admin system through the use of their own passwords; they will only have access to their own data, unless they hold a role within the Society which requires wider access (such as the Membership Secretary). Any requests for data to be updated will be processed within one month.
- *Right to object:* Individuals can object to their data being used for a particular purpose. ACS will always provide a way for an individual to withdraw consent in all marketing communications. Where we receive a request to stop using data we will comply unless we have lawful reason to use data for legitimate interests of contractual obligation.
- *Right to erasure:* Individuals can request for all data held on them to be deleted. ACS's data retention policy will ensure that data is not held for longer than is reasonably necessary in relation to the purpose it was originally collected. If a request for deletion is made we will comply with the request unless:
    - There is a lawful reason to keep and use the data for legitimate interests or contractual obligation.
    - There is a legal requirement to keep the data.
- *Right to restrict processing:* Individuals can request that their personal data be 'restricted' – that is, retained and stored but not processed further (e.g. if they have contested the accuracy of any of their data. ACS will restrict the data while it is verified).

Though unlikely to apply to the data processed by ACS, we will also ensure that rights related to portability and automated decision making (including profiling) are complied with where appropriate.

Member-to member and ACS supports' contact

We only share members' data with other members with the subject's prior consent.

As a membership organisation, on the other hand, ACS encourages communication between members. To facilitate this:

- Members can request the personal contact data of other members in writing via the DPO or Membership Secretary. These details will be given, as long as they are for the purposes of contacting the subject (e.g. an email address; not financial or health data) and the subject has consented to their data being shared with other members in this way.
- ACS will regularly collect data from consenting supporters (e.g. supporters of ACS who have consented to be on a mailing list for marketing purposes). This includes contacting them to promote performances, updating them about group news, fundraising and other group activities.
- Any time data is collected for this purpose (see the previous bullet point), we will provide:
    - A method for users to show their positive and active consent to receive these communications (e.g. a 'tick box');
    - A clear and specific explanation of what data will be used for (e.g. to promote performances).
- Data will only ever be used in the way described and consented to.
- Every marketing communication will contain a method through which a recipient can withdraw their consent. Opt-out requests will be processed within 14 days.

Data breaches

ACS takes any breach of data seriously. A data breach could be deliberate or accidental:

- Loss of data, including devices being lost or stolen;
- Destruction of data, both physical and digital;
- Corruption of data (e.g. changing data without permission or good reasons, or changing it with permission or good reason but incorrectly, either by ACS staff, volunteers or third parties;
- Unauthorised use of data;
- Unauthorised access to data;
- Unauthorised disclosure of data.

ACS acknowledges that a data breach can occur through both action and inaction on the part of the Data Controller or Processor.

(1) How we prevent data breaches

ACS has the following safeguards to ensure against possible data breaches:

- Data is stored on secure systems with access controlled by passwords;
- Automatic, and manual, processes ensure passwords are updated on a regular basis, including as soon as an individual's role within, or relationship to, ACS chnges;
- Automatic and manual processes ensure mass communications are only sent in line with mailing prefrences.

(2) If a data breach occurs

If anyone associated with ACS thinks a data breach has occurred then it should be reported to the DPO / committee immediately.
The DPO / committee will work with relevant individuals to investigate the potential breach. The response plan will include the following steps:

- Establish if a breach has occurred;
- Investigate if any measure can be taken to contain or minimise the breach;
- Establish the full extent and nature of that breach – including what the breach was, how many data subjects are affected and who they are;
- Establish if the data breach has posed, or is likely to pose a significant risk to the data subjects' rights and freedoms:
    - If the breach does pose a significant risk to the data subjects' rights and freedoms, we will:
        - Ensure all committee members (trustees) are informed.
        - Report the breach to the Information Commissioner's Office (ICO). This will be done in line with their guidelines and as soon as possible, but no later than 72 hours after the breach occurred.
        - Report the breach to any other relevant regulators, including the Charity Commission.
        - Report the breach to the data subjects affected, informing them of what has happened, possible and likely impacts it might have on them and what we are doing to manage the breach and reduce risk of future occurrences.
    - If the breach does not pose a significant risk to the data subjects' rights and freedoms, we will:
        - Document details of the breach and the decision making process involved in assessing the severity and risk of the breach.
        - Ensure the breach is reported to the Committee / Trustees at the next planned full committee meeting.

Conduct an internal investigation into how the breach happened and what measures need to be taken to minimise the risk of similar breaches occurring in the future.

Cookies on the ACS website

A cookie is a small text file that is downloaded onto 'terminal equipment' (e.g. a computer or smartphone) when the user accesses a website. It allows the website to recognise that user's device and store some information about the user's preferences or past actions.

ACS uses cookies on our website (https://www.aylesburychoral.org.uk) in order to monitor and record users' activity. This allows us to improve users' experience of our website by, for example, allowing for a 'logged in' state and by giving us useful insight into how users as a whole are engaging with the website.

We will implement a pop-up box on the website that will activate each new time a user visits the website. This will allow them to click to consent (or not) to continuing with cookies enabled, or to ignore the message and continue browsing (i.e. give their implied consent).

It will also include a link to our Privacy Policy which outlines which specific cookies are used and how cookies can be disabled in the most common browsers.

Data retention policy

Introduction

This policy sets out how the Society will approach data retention and establishes processes to ensure we do not hold data for longer than is necessary.

It forms part of the Society's Data Protection Policy.

Roles and responsibilities

Aylesbury Choral Society is the Data Controller and will determine what data is collected, retained and how it is used. The Data Protection Officer (DPO) for ACS is the chairman or, when the chair is not available, the webmaster. However, membership data (e.g. name and contact details) is also collected by the Membership Secretary and financial data (e.g. details of 'subs' paid) by the Society's Treasurer. The DPO together with Society's committee are responsible for the secure and fair retention and use of data by ACS. Any questions relating to data retention or use of data should be directed to the DPO.

A regular review of all data will take place to establish if ACS still has good reason to keep and use the data held at the time of the review.

As a general rule a data review will be held every two years and no more than 27 calendar months after the previous review. The first review will take place on or shortly after **1st September 2027**.

Data to be reviewed

- ACS stores data on digital documents (e.g. spreadsheets) stored on personal devices held by committee members.
- Data stored on third-party online services (e.g. Making Music).
- Physical data stored at the homes of committee members.

Who the review will be conducted by

The review will be conducted by the DPO with other committee members to be decided at the time of the review.

How data will be deleted

- Physical data will be destroyed safely and securely, including shredding
- All reasonable and practical efforts will be made to remove data stored digitally.
    - Priority will be given to any instances where data is stored in active lists (e.g. where it could be used) and to sensitive data.
    - Where deleting the data would mean deleting other data that we have a valid lawful reason to keep (e.g. on old emails) then the data may be retained safely and securely but not used.

Criteria

The following criteria will be used to make a decision about what data to keep and what to delete:

Question	**Action**	
	Yes	**No**
Is the data stored securely?	No action necessary	Update storage protocol in line with Data Protection 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	Ask the subject to confirm/update details
Where appropriate do we have consent to use the data. This consent could be implied by previous use and engagement by the individual	Continue to use	Get consent
Can the data be anonymised	Anonymise data	Continue to use

Statutory requirements

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

- Gift Aid declarations records
- 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
- Tax and employment records

Member data

- When a member leaves ACS and all administrative tasks relating to their membership have been completed, any potentially sensitive data held on them will be deleted – this might include, for example, bank details.
- Unless consent has been given data will be removed from all emailing lists.
- All other data will be stored safely and securely and reviewed as part of the next two-year review.

Mailing list data

- If an individual opts out of a mailing list, their data will be removed as soon as is practically possible.
- All other data will be stored safely and securely and reviewed as part of the next two-year review.

Volunteer and freelancer data

- Whan a volunteer or freelancer stops working with ACS and all administrative tasks relating to their work have been completed, any potentially sensitive data held on them will be deleted (e.g. bank details).
- Unless consent has been given, data will be removed from all email mailing lists.
- All other data will be stored safely and securely and reviewed as part of the next two-year review.

Other data

- All other data will be included in a regular two-year review.

Policy established: June 2025
Last reviewed: July 2025