Fleet Choral Society (FCS) Data Protection Policy

Scope of the policy

This policy applies to the work of FCS. The policy sets out the requirements that FCS has in order 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 FCS committee members to ensure that we are compliant. This policy should be read in tandem with FCS's Privacy Policy.

Why this policy exists

This data protection policy ensures FCS:

- 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 and Section Leaders (SLs)

- 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 FCS.
- FCS will provide induction training to committee members and SLs to help them understand their responsibilities when handling data.
- Committee Members and SLs 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. Files such as Word and Excel data should be password encrypted wherever possible.
    - Data should not be shared outside of the FCS unless with prior consent and/or for specific and agreed reasons. Examples would include Gift Aid information provided to HMRC or information provided to travel agents in connection with overseas tours.
    - Member information should be refreshed periodically to ensure accuracy, via the membership renewal process or when policy is changed.

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 if personal data is inaccurate, having regard to the purposes for which it is processed; if necessary it should be 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 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 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

FCS requests personal information from potential members and members for membership applications and for sending communications about their involvement with the FCS. 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 for what the information will be used. The lawful basis for obtaining member information is due to the contractual relationship that the FCS has with individual members. In addition, members will be asked to provide consent for specific processing purposes. FCS members will be informed as to whom they need to contact should they wish their data not to be used for specific purposes for which they have previously provided consent. Where these requests are received they will be acted upon promptly and the member will be informed when the action has been taken place.

Processed for specified, explicit and legitimate purposes

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

- Communicating with members about FCS events and activities.
- Section Leaders communicating with group members about specific group 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.

FCS will ensure that Section Leaders are made aware of what would be considered appropriate and inappropriate communication. Inappropriate communication would include sending FCS members marketing and/or promotional materials from external service providers.

FCS will ensure that members' information is managed in such a way as not to infringe an individual member’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

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

- Name
- Postal address
- Email address
- Telephone number
- Gift Aid eligibility

Where additional information may be required such as health related information this will be obtained with the consent of the member who will be informed as to why this information is required and the purpose for which it will be used. At present FCS does not collect or envisage collecting any members' health information.

Where FCS organises a trip or activity that requires, or where we suggest, 'next of kin' or 'In Case of Emergency' (ICE) information be provided, a form requesting the members consent will need to be completed in order to document the information and the members signature.

Photographs

Photographs are classified as personal data. Where group photographs are being taken members will be asked to step out of shot if they do not wish to be in the photograph. Otherwise verbal consent will be obtained from members in order for photographs to be taken and members will be informed as to where photographs will be displayed. Should a member wish at any time to remove their consent and to have their photograph removed then they should contact person who took the photograph to advise them that they no longer wish their photograph to be displayed.

Accuracy of data and keeping data up-to-date

FCS 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. In addition, on an annual basis, the membership renewal process will provide an opportunity for members to inform FCS of any changes in their personal information.

Accountability and governance

The FCS Committee are responsible for ensuring that the FCS remains compliant with data protection requirements and keeping evidence that it has. Where consent is required for specific purposes then evidence of this consent (either electronic or paper) will be obtained and retained securely. The FCS Committee will ensure that new members joining the Committee receive an induction into the requirements of GDPR and the implications for their role. FCS will also ensure that Section Leaders are made aware of their responsibilities in relation to the data they hold and process. 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 and Section Leaders relinquish their roles, they will be asked to either pass on data to those who need it and/or delete data.

Secure Processing

FCS Committee Members and Section Leaders (SLs) have a responsibility to ensure that data is both securely held and processed. This will include:

- Committee members and SLs using strong passwords

- Committee members and SLs not sharing passwords
- Restricting access to member information to those on the Committee who need to communicate with members on a regular basis
- Using strong password protection on laptops and PCs that contain personal information for FCS members

Subject Access Request

FCS members are entitled to request access to the information that is held by FCS. The request needs to be received in the form of a written request to the Membership Secretary of the FCS. 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. FCS 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 FCS 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 FCS members to inform them of the data breach and actions taken to resolve the breach.

Where a FCS member feels that there has been a breach by the FCS, 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 FCS 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 notified of the outcome.

This policy is to be read in conjunction with the FCS Privacy Policy.

Approved by FCS June 8th 2021

Policy review date: June 2022