Harrisburg Gay Men's Chorus
Data Protection and Security Policy

Statement of policy and purpose of Policy

1. **Harrisburg Gay Men's Chorus** (known hereafter as "***Chorus***") is committed to ensuring that all personal information handled by us will be processed accordingly to legally compliant standards of data protection and data security.
2. The purpose of this policy is to help us achieve our data protection and data security aims by:
   a. notifying subjects of the types of personal information being retained by the Chorus, and what the Chorus does with that information;
   b. ensuring all Chorus Members understand our rules and the legal standards for handling personal information;
   c. clarifying the responsibilities and duties of members in respect of data protection and data security.
3. This is a statement of policy only. This policy may be amended at any time at the discretion of the Harrisburg Gay Men's Chorus Board of Directors (known hereafter as "***Board of Directors***").

Who is responsible for data protection and data security?

4. Maintaining appropriate standards of data protection and data security is a collective task shared between the Board of Directors and Chorus Members. This policy and the rules contained in it apply to all Chorus Members, irrespective of their position within the Chorus.
5. The Board of Directors has overall responsibility for ensuring that all personal information is handled in compliance with the law and has appointed a member of the Information Technology committee as the ***Data Protection Officer*** with day-to-day responsibility for data processing and data security.
6. All Chorus Members have responsibility to ensure compliance with this policy, to handle all personal information consistently with the principles stated herein, and to ensure that measures are taken to protect the data security. The Board of Directors has special responsibility for leading by example and to monitor and enforce compliance.
7. Any breach of this policy will be taken seriously and may result in disciplinary action.

What personal information and activities are covered by this policy?

8. This policy covers personal information collected, provided or gathered in the course of normal business operations of the Chorus:
   a. which relates to a living individual who can be identified either from that information in isolation or by reading it together with other information possessed by the Chorus;
   b. is stored electronically or on paper in a filing system;
   c. in the form of statements of opinion as well as facts;
   d. which relates to Members (present, past or future), Patrons, Benefactors, Volunteers, Vendors or to any other individual whose personal information the Chorus may handle or control (collectively known as "***Subjects***");
   e. obtained, held or stored, organized, disclosed or transferred, amended, retrieved, used, handled, processed, transported or destroyed.
9. The types of personal information the Chorus may collect, store and use about individual Subjects include records relating to their:
   a. home address and contact details as well as contact details for their next of kin, when applicable;
   b. subscription records, including detailed contribution, advertising, gift or donations made to or in favor of the Chorus;
   c. attendance records at rehearsals and concerts;
   d. member voice range, when applicable;
   e. telephone, email; gender;
   f. member date of birth; - for social and insurance purposes;
   g. recordings of rehearsals and concerts, photos and videos, which may be posted to Chorus owned and operated web sites and social media sites for the purposes of promoting the Chorus and its activities.
10. The Chorus will use information to carry out our normal business activities, to administer membership and to deal with any problems or concerns that may exist including:
    a. a database which is used to compile and maintain lists of home and/or business address and contact details, for the purposes of marketing and solicitation of charitable contributions;
    b. attendance records: to maintain a record of member attendance in order to ascertain eligibility to perform at any of the Chorus's concerts;

c. administration of member use and access of Information Technology resources (e.g. Chorus portal);
d. complaint, grievance or legal matters: in connection with any complaint, grievance, legal, regulatory or compliance matters or proceedings that may involve a Chorus member;
e. maintenance of adequate records for the efficient operation of the Chorus.

11. Confirming that for the purposes of the **Federal Trade Commission Act (15 U.S.C. §§41-58)**, the Board of Directors is a Data Controller of the personal information in connection with all Entity information. This means that the Board of Directors will determine the purposes for which, and the manner in which, personal information is obtained and processed.
12. The Chorus will take reasonable steps to ensure that all Subject information is kept secure, as described later in this policy and in general, Subject information will not be disclosed to others outside the Chorus, except:.
    a. to comply with our legal obligations or assist in a criminal investigation or to seek legal or professional advice in relation to Subject issues, which may involve disclosure to our lawyers, accountants or auditors and to legal and regulatory authorities, such as the Internal Revenue Service;
    b. to other parties which provide products or services to us. (e.g. insurance services or service providers).
13. By providing personal information to us, Subjects consent to the use of personal information (including any sensitive personal data) in accordance with this policy.

Data Protection Principles.

14. Chorus members whose work involves using personal data relating to Subjects must comply with this policy and with the eight legal data protection principles which require that personal information is:
    a. processed fairly and lawfully. The Chorus must always have a lawful basis to process personal information. In most (but not all) cases, the person to whom the information relates (the Subject) must have given consent. The Subject must be told who controls the information (the Board of Directors), the purpose(s) for which the Chorus is processing the information and to whom it may be disclosed;
    b. processed for limited purposes and in an appropriate manner consistent with which the initial consent was obtained;
    c. adequate, relevant and not excessive for the purpose;
    d. accurate. Regular checks must be made to correct or destroy inaccurate information;
    e. not kept longer than necessary for the purpose. Information must be destroyed or deleted when no longer required or appropriate for business purposes;
    f. processed in line with Subjects' rights. Subjects have a right to request access to their personal information, prevent their personal information being sold or disclosed to a third-party, request the correction of inaccurate data and to prevent their personal information being used in a way likely to cause them or another person damage or distress;
    g. secure. See further information about data security below;
    h. not transferred to people or organizations without adequate protection.
15. Some personal information needs even more careful handling. This includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life or about criminal offences. Strict conditions apply to processing this sensitive personal information and the Subject must normally have given specific and express consent to each way in which the information is used.

Data security.

16. The Data Protection Officer must protect personal information in our possession from being accessed, lost, deleted or damaged unlawfully or without proper authorization through the use of data security measures.
17. Maintaining data security means making sure that:
    a. only people who are authorized to use the information can access it;
    b. information is accurate and suitable for the purpose for which it is processed;
    c. authorized persons can access information if they need it for authorized purposes. Members should make every effort to securely store personal data on computer systems.
18. By law, the Chorus must use procedures and technology to secure personal information throughout the period that the information is held or controlled, from the time period in which the information is obtained until said information is destroyed.

19. Personal information must not be transferred to any person to process (eg while performing services for us on or our behalf), unless that person has either agreed to comply with our data security procedures or the Chorus is satisfied that other adequate measures exist.
20. Security procedures include:
    a. physically securing information. Computers should be locked with a password or shut down when they are left unattended and discretion should be used when viewing subject information on a monitor to ensure that it is not visible to others. Memory stick or other external memory devices containing Subject data must be kept secure.
21. Electronic Request Precautions. Particular care must be taken to avoid inappropriate disclosures:
    a. no electronic requests (including telephone, fax, email or social media) for disclosure of Subject information shall be honored. All information requests must be provided in writing and addressed to the Board of Directors.
22. Methods of disposal. Copies of Subject information, whether on paper or on any physical storage device, must be physically destroyed when they are no longer needed. Paper documents should be shredded and CDs or memory sticks or similar must be rendered permanently unreadable.
23. Additional measures to ensure data security include the Subject database be password protected and will be available only to those members of the Chorus as required in execution of their duties.

Subject access requests.

24. By law, any Subject (including Members) may make a formal request for information that the Chorus holds about them, provided that certain conditions are met. The request must be made in writing.
25. Any written request for Subject information disclosure should be immediately forwarded to the Board of Directors.