HHCOS Data Protection Policy
November 2020

Introduction

The General Data Protection Regulation (GDPR) is a new, Europe-wide law that replaces the Data Protection Act 1998 in the UK. The GDPR sets out requirements for how organisations must process personal data from 25 May 2018.

Scope of the policy

This policy governs the processing of personal data by Haddo House Choral & Operatic Society according to the terms of the GDPR. This policy and the guidelines laid down to enact it must be complied with at all times by anyone in the Society who holds and processes the personal and sensitive information of choral members, child members, Friends, supporters, partners or contractors. The reason for this is two-fold:

- To protect individuals from having their personal and sensitive data misused.
- To protect HHCOS volunteers and office-bearers from personal and collective criminal liability. Failure to comply with the policy may result in legal proceedings against the individual and/or the Society.

Definitions

- *Personal data* means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.
- *The Data Controller* determines the purposes and means of processing personal data. The GDPR places obligations on the data controller (HHCOS) to ensure contracts with processors comply with the GDPR.
- The *Data Protection Officer* will oversee and advise on the compliance with the GDPR by members of the society.
- A *data processor* is responsible for processing personal data on behalf of a controller. If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.

- This policy applies to data in all forms: paper copies, electronic data held on phones, laptops, computers, memory sticks, external drives, or shared in social messaging applications.

Data Controller:	Haddo House Choral and Operatic Society
Data Protection Officer:	Management Committee Members
Data Processors:	All office holders who hold and process personal data.

Key principles

These key principles as defined by the GDPR will govern the HHCOS Data Protection Policy and guidelines.

1. *Lawfulness, fairness and transparency:* we have a lawful basis for collecting data; we will process the data in a way that is not detrimental or misleading to the individual; we will be clear, open and honest with people about how we use their personal data.
2. *Purpose limitation:* we clearly identify the purpose for processing data.
3. *Data minimisation*; the data we process is adequate, relevant and not excessive.
4. *Accuracy*: we will ensure the accuracy of any personal data we create and keep updated.
5. *Storage limitation*: we will not keep the data for longer than we need it. We will set standard retention periods wherever possible and erase any data no longer required.
6. *Integrity and confidentiality (security):* we will keep data secure by means of appropriate technical and organisational measures
7. *Accountability:* we will have appropriate measures and records in place to demonstrate our compliance with the GDPR principles

These principles will be underpinned by the following actions and guidelines:

Informing individuals of their rights

The updated Privacy Statement sets out clearly and honestly to individuals (Members, Friends, Patrons, Supporters, Contractors, Partners etc) why we are collecting personal data, and on what basis. This document will be made available to all individuals who submit their personal data to the Society, whether via our website, email or in writing.

A brief, specific Privacy Notice will also be appended to all correspondence and proformas, to ensure that individuals understand their rights when they are consenting to giving their personal data to the Society.

Access to personal data

Every data subject has the right to request a copy of the information held about him or her. This includes information in databases, forms and in some cases emails. For any request received reasonable effort must be made to collate all information held about that individual.

All requests for Data Access must be referred to the Data Protection Officer who will coordinate the collation of data and subsequent response. Requests for Data Access must be made in writing along with a copy of one of the following forms of identification. Permitted forms of identification are: Drivers Licence, Utility Bill, Bank Statement, Passport(if accompanied with a form of identification showing address). Responses will only be sent to the address detailed on the item of identification.

Ensuring accuracy

Data will be regularly updated by office-holders. Reasonable steps must be taken to ensure the data held by the Society is accurate.

- Data should be initially obtained from the individual (or their representative) and not via a third party.
- If data is to be retained for an extended period of time it should be validated as correct at least every 2 years.
- Information that is retained and frequently used must be available to the individual subject for them to check and update.

Storage limitation

Data should not be retained any longer than necessary. Individuals do have a right to challenge retention of their data and a right to erasure if we no longer need it.

The following should be used as a guideline for retention periods; however, specific guidance should be agreed and advised upon by the Data Controller, ie Management Committee.

Purpose of data retention	Storage limitation
Ticket orders	30 days after the event
Membership information, Friends information, 200 club subscribers' information (excluding financial data where required for auditing purposes)	Retained for the duration of the contract and afterwards for an indefinite period for notification of events/performances and related information, unless requested otherwise.
Financial information: e.g. Gift Aid	As required by HMRC for auditing purposes
Post event feedback	30 days after the event

Some personal data may be retained longer for a specific purpose, eg:
Financial data: where information is required for accounting procedures, auditing or as evidence for the Charities Commission, the data should be retained in accordance with statutory requirements.

Where permission has been granted for the Society to retain the data for an extended period of time (eg marketing, mailing lists) data may be retained until permission is revoked. When such notification is received, data must be disposed of within 2 weeks.

Archive and public interest/statistical information: limited personal data may be kept for longer for archiving purposes, eg for the purpose of historical interest in the Society. Such data should be limited and anonymised where possible.

Ensuring secure communication

- Communication with individuals on any HHCOS business should only be via secure, web-based, HHCOS-owned email accounts @hhcos.org.uk), eg: performancecommittee@ chairman@, etc. These email accounts will be accessible to the current post-holder and other designated committee members, and to the web administrator. Once office-holders leave office, they should wipe files and no longer have access to these accounts.
- Email correspondence MUST use BCC (blind carbon copy) for circulation lists/group emails.
- Extreme care should be taken not to use 'Reply All' or to inadvertently forward email strings, as this could breach confidentiality.

- Communications with children under 16 years (or where an adult at risk of harm has a legal guardian) must be via the parent or guardian, or should always have another appropriate adult office-holder copied into the email (DSO, Deputy DSO or Chairman). Parents/guardians and young people should be made aware of this protocol and reminded where required.
- Where group apps or social media (eg Whatsapp, Facebook, Twitter) are used for communications, this must only be used for **parents/guardians** of under 16s, and never directly with children under 16 years. It must never be used for communicating identifying personal information for individuals of any age, eg names, contact details, date of birth, specific arrangements.
- Permission must be obtained from individuals (or parents/guardians of under 16s or adults at risk of harm with a legal guardian) for taking photos or publishing photos. This permission is requested on the membership form.

Ensuring secure storage

Data must be stored in a secure fashion.

- Paper Records must be stored in a locked storage container such as a safe, lockable filing cabinet or locked records box.
- Electronic Records containing sensitive information must be secured using a pin code or complex password.

Disposal of Data

Data must be disposed of in a secure fashion.

Paper Records – these should be machine-shredded prior to disposal through normal household waste. If access to a shredder or burner is not available, records should be passed to the Data Protection Officer for appropriate disposal. Records must not be torn by hand.

Electronic Records – reasonable steps should be taken to remove electronic data from all areas of storage.

Initially data should be deleted using normal Operating System procedures. If the equipment upon which the data was held is to be disposed of (including by sale or gift) measures should be taken to securely wipe the hard disk drive. Guidance on removal of electronic data can be sought from the Data Protection Officer.

Ensuring good practice and accountability in HHCOS

- Committee members should be briefed upon joining the committee on their responsibilities with regard to Data Protection and Privacy.
- Training and awareness raising will be carried out for all Committee members and others who hold personal or sensitive data when required.
- An annual data audit will be carried out and any immediate issues will be addressed.
- Sharing of information will be limited to those individuals who need the specific information to carry out the duties of their office and this information will not be shared as standard practice.
- When office-holders vacate their post they will be asked to hand back personal information for passing on to their successors, or for shredding. They will be asked to ensure that their electronic devices have been cleared of all personal data they have held while in office. This includes any emails in inbox or sent folders.
- Where particular sets of data are created for a specific event, eg an opera, then this should be destroyed after the event unless there is a clear and justifiable reason to keep it (as agreed by the Data Protection Officer).

Loss of Data or Breach of the Policy

In the event of any loss of data or breach of the policy, the Data Controller and the Chairperson of the Society must be notified immediately as there is a legal requirement to report the loss to the Information Commissioner's Office where required according to their guidelines within a specified time period.

Individual members of HHCOS may be held criminally liable for personal actions that breach the Society's data protection policy and organizational guidelines.

November 2020

We are committed to reviewing our policy and good practice annually.
This policy was reviewed on: November 2020
Signed: …… Chairman, HHCOS