HANDBELL RINGERS OF GREAT BRITAIN

(including all HRGB Events, HRGB Sales, William Hartley Memorial Fund, Vaughan Evans Fund, and HRGB Promotions Ltd.)

Data Protection Policy

Policy Date June 2018

CONTENTS

1. Overview
2. Data Protection Principles
3. Personal Data
4. Special Category Data
5. Processing
6. How personal data should be processed
7. Privacy Notice
8. Consent
9. Security
10. Sharing personal data
11. Data security breaches
12. Subject access requests
13. Data subject rights
14. Contacts
15. Review

Data Protection Policy

1 Overview

1.1 Handbell Ringers of Great Britain (subsequently denoted as HRGB) takes the security and privacy of personal information seriously. As part of our activities we need to gather and use personal information about our members (ordinary, independent and honorary) and office-holders. The Data Protection Act 2018 (the "2018 Act") and the EU General Data Protection Regulation ("GDPR") regulate the way in which personal information about living individuals is collected, processed, stored or transferred.

1.2 This policy explains the provisions that we will adhere to when any personal data belonging to or provided by data subjects, is collected, processed, stored or transferred on behalf of HRGB.

1.3 HRGB has a separate Privacy Notice which outlines the way in which we use personal information provided to us. A copy can be obtained on the HRGB website.

1.4 All personal data must be held in accordance with HRGB's Data Retention Policy, which must be read alongside this policy. Data should only be held for as long as necessary for the purpose for which it is collected.

1.5 This policy does not form part of any contract for services and can be amended by HRGB at any time. It is intended that this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, HRGB intends to comply with the 2018 Act and the GDPR.

1.6 Any deliberate or negligent breach of this policy by a member of HRGB is a very serious matter. It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see paragraph 12 below) and such conduct by an office-holder would amount to gross misconduct.

2 Data Protection Principles

2.1 It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted, destroyed or rectified without delay;
- not be kept for longer than is necessary for the purpose for which it is processed;
- be processed securely

HRGB is accountable for these principles and must be able to demonstrate compliance.

3 Definition of personal data

3.1 "Personal data" means information which relates to a living person (a "data subject") who can be identified from that data on its own, or when taken together with other information which is likely to come into the possession of the data controller. It does not include anonymised data.

3.2 This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

4 Definition of special categories of personal data

4.1 "Special categories of personal data" are types of personal data consisting of information revealing: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic or biometric data; health; sex life and sexual orientation; and any criminal convictions and offences.

4.2 Some personal data held by HRGB will be classed as special category personal data - health data held in some instances and bank details of members.

5 Definition of processing

5.1 "Processing" means any operation which is performed on personal data, such as collection, recording, organisation, structuring or storage; adaption or alteration; retrieval, consultation or use; disclosure by transmission, dissemination or otherwise making it available; and restitution, destruction or erasure.

6 How personal data should be processed

6.1 Everyone who processes data on behalf of HRGB has responsibility for ensuring that the data they collect and store are handled appropriately, in line with this policy, our Data Retention Policy and our Privacy Notice.

6.2 Personal data should only be accessed by those who need it for the work they do for or on behalf of HRGB. Data should only be used for the specified lawful purpose for which it was obtained.

6.3 The legal basis for processing personal data (other than special category data, which is referred to in paragraph 8 below) is that the processing is necessary for the purposes of HRGB's legitimate interests.

6.4 Personal data held in all manual files and databases should be kept up to date. It should be shredded or disposed of securely when it is no longer needed. Unnecessary copies of personal data should not be made.

7 Privacy Notice

7.1 If HRGB's use of personal data is what someone would reasonably expect, we will provide information about this using a Privacy Notice which will be available on the HRGB website.

8 When is consent needed for the processing of personal data?

8.1 Some personal data held by HRGB will be classified as special category personal data as it may give information about the member's health or banking details.

8.2 Processing of such special category data is prohibited under the GDPR unless one of the listed exemptions applies. The relevant one for HRGB is that "the individual has given **explicit consent** to the processing of the personal data for one or more specific purposes"

8.3 Where personal data are to be shared with a third party, HRGB will only do so with the explicit consent of the data subject. For example, personal data will only be included in a directory for circulation to the general public or included on a website accessed by the general public where consent has been obtained.

8.4 If consent is required to process the information this should be recorded using a consent form. If consent is given orally rather than in writing, this fact should be recorded in writing.

9 Keeping personal data secure

9.1 Personal data should not be shared with those who are not authorised to receive it. Care should be taken when dealing with any request for personal information over the telephone or otherwise. Identity checks should be carried out if giving out information to ensure that the person requesting the information is either the individual concerned or someone properly authorised to act on their behalf.

9.2 Hard copy personal information should be stored securely (in lockable storage, where appropriate) and not visible when not in use. Filing cabinets and drawers and/or office doors should be locked when not in use. Keys should not be left in the lock of the filing cabinet/lockable storage.

9.3 Passwords should be kept secure, should be strong, changed regularly and not written down or shared with others.

9.4 Emails containing personal information should not be sent to or received at a work email address as this might be accessed by third parties.

9.5 The "bcc" rather than the "cc" or "to" fields should be used when emailing a large number of people, unless everyone has agreed for their details to be shared amongst the group.

9.6 Personal data should be encrypted or password-protected before being transferred electronically or sent via a secure system such as Norton "wifi privacy".

9.7 Personal data should never be transferred outside the European Economic Area except in compliance with the law or with the explicit consent of the data subjects involved.

10 Sharing of information

10.1 HRGB will only share someone's personal data where we have a legal basis to do so, including for our legitimate interests within HRGB. We may share information with recognised companies (who are compliant with the GDPR regulations) to enable the mailing of Reverberations, regional newsletters and details of events either by post or

electronically to our members. Personal data will be shared with HMRC to enable the reclamation of Gift Aid where a member has requested this. Personal information may also be shared with third parties essential to the running of an event e.g. dietary requirements to caterers. In the case of a medical emergency any medical and other personal details will be shared with emergency services.

10.2 HRGB will not send any personal data outside the European Economic Area unless with the explicit consent of the data subjects involved. If this changes all individuals affected will be notified and the protections put in to secure your personal data, in line with the requirements of the GDPR.

11 How to deal with data security breaches

11.1 Should a data security breach occur, the NEC office bearer, or Regional office bearer who identifies the breach will notify the HRGB Data Controller immediately. If the breach is likely to result in a risk to the rights and freedoms of individuals then the Information Commissioner's Office must be notified within 72 hours.

12 Subject access requests

12.1 Data subjects can make a subject access request to find out what information is held about them. This request must be made in writing. Any such request received by HRGB will be responded to by the Data Controller within the necessary time limit (30 days).

12.2 It is a criminal offence to conceal or destroy personal data which is part of a subject access request.

13 Data subject rights

13.1 Data subjects have certain other rights under GDPR. These include the right to know what personal data HRGB processes, how it does so and what is the legal basis for doing this.

13.2 Data subjects also have the right to request that HRGB corrects any inaccuracies in their personal data, and erase their personal data where it is not entitled by law to process it or it is no longer necessary to process it for the purpose for which it was collected. Data should be erased when an individual revokes their consent in situations where explicit consent was obtained (and consent is the basis for processing); when the purpose for which the data was collected is complete; and when compelled by law.

13.3 All requests to have personal data corrected or erased should be forwarded to HRGB's Data Controller who will be responsible for responding to them.

14 Contracts

14.1 If any processing of personal data is to be outsourced from HRGB we will ensure that the mandatory processing provisions imposed by the GDPR will be included in the agreement or contract.

15 Policy review

The National Executive Committee (NEC) will be responsible for reviewing this policy from time to time and updating HRGB in relation to its data protection responsibilities and any risks in relation to the processing of data.

Review date June 2020

Handbell Ringers of Great Britain

Data Retention Policy

1 Introduction

1.1 HRGB at national and regional level gathers personal information from members and external organisations as well as generating a wide range of personal data, all of which is recorded in documents and records, both in hard copy and electronic forms.

1.2 Examples of the types of information accumulated and generated are set out in Appendix 1 of this policy and include but are not limited to minutes of committee meetings, membership lists, newsletters, Reverberations, medical information, bank details of NEC and regional members, dietary requirements and other communications such as letters and emails.

1.3 In certain circumstances it will be necessary to retain documents to meet legal requirements and for operational needs. Document retention is also required to evidence agreements or events and to preserve information.

1.4 It is however not practical or appropriate for HRGB to retain all records. Additionally, data protection principles require information to be as up to date and accurate as possible. It is therefore important that HRGB has in place systems for the timely and secure disposal of documents that are no longer required.

1.5 This Data Retention Policy was adopted by HRGB on 23rd June 2018 and will be implemented on a day to day basis.

2 Roles and Responsibilities

2.1 Office holders will adopt the retention and disposal guidance at Appendix 1 of this policy and strive to keep records up to date.

3 Retention and Disposal Policy

3.1 Decisions relating to the retention and disposal of data should be guided by:-

3.1.1 Appendix 1 - Document Retention Schedule - Guidance on the recommended and statutory minimum retention periods for specific types of documents and records.

3.1.2 Appendix 2 - Quick Guide to document retention.

3.2 In circumstance where the retention period for a specific document or category of documents has expired, a review should be carried out prior to disposal and consideration should be given to the method of disposal.

4 Disposal

4.1 Documents containing confidential or personal information should be disposed of either by shredding or by using confidential waste bins or sacks. Such documentation is likely to include banking details of NEC or regional members, contact lists with names and addresses, medical details and dietary requirements.

4.2 Documents other than those containing confidential or personal information may be disposed of by recycling or binning.

4.3 Electronic communications including email, Facebook pages, twitter accounts etc and all information stored digitally should also be reviewed and if no longer required, closed and/or deleted so as to be put beyond use. This should not be done simply by archiving, which is not the same as deletion. It will often be sufficient simply to delete the information, with no intention of ever using or accessing it again, despite the fact that it may remain in the electronic ether. Information will be deemed to be put beyond use if HRGB is not able, or will make no attempt, to use it to inform any decision in respect of any individual or in a manner that affects the individual in any way and does not give any other organisation or individual access to it.

4.4 Deletion can also be effected by using one of the following methods of disposal:-

- Using secure deletion software which can overwrite data;
- Using the function of “restore to factory settings”(where information is not stored in a removable format);
- Sending the device to a specialist who will securely delete the data.

Appendix 1

Illustrative Data Retention Schedule

This Schedule is provided as a guide to the minimum length of time that certain documents should be retained in case of questions or legal issues arising from them. It is not part of the GDPR regulations or the HRGB data protection policy and it does not imply that any listed documents MUST be destroyed after the given period of time.

Much HRGB documentation is stored in the national and regional archives.

Avoid retaining information if there is no reason for doing so.

RECORD	MINIMUM RETENTION PERIOD
Minutes of Annual General Meetings	50 years
Minutes of committee meetings (NEC and Regional)	6 years
Membership Register	Reviewed annually, delete out of date information
Databases for mailing lists / distribution	Reviewed annually, delete out of date information
Miscellaneous contact information (non members)	Delete once there is no longer a requirement to hold such information
Documents relating to litigation or potential litigation	Until matter is concluded plus 6 years
Injury and Illness Incident Reports (RIDDOR)	5 years
Contracts	6 years following expiration
Fixed Asset Records	Permanent
Application for charitable and / or tax-exemption status	Permanent
Sales and Purchase records	5 years
Resolutions	Permanent
Charities Commission and OSCR filings	5 years from date of filing

Records of financial donations	6 years
Accounts Payable and Receivables ledgers and schedules	6 years
Annual examination reports and financial statements	Permanent
Annual plans and budgets	2 years
Bank statements, cancelled cheques, deposit slips	Minimum of 6 years
Trustee expense records	6 years
Cash receipts	3 years
Cheque registers	Permanent
Electronic fund transfer documents	6 years
General ledgers	Permanent
Invoices	6 years
Tax records	Minimum of 6 years
Filings of fees paid to professionals	6 years
Insurance claims / applications	Permanent
Insurance disbursements and denials	Permanent
Insurance contracts and policies	Permanent
Warranties	Duration of warranty plus 6 years
Records relating to potential, or actual, legal proceedings	Conclusion of any proceedings plus 6 years
WHMF loan agreements, loan records, letters of thanks to Patron and Standing Committee	6 years then store in archive as items of historical interest

Appendix 2

General guidance for documents NOT included in the retention schedule.

On-going business use is subjective, but generally refers to documents still required for on-going activities or projects, or documents that may still need to be referred to for on-going activities.