EMMS International

Health for Today, Hope for Tomorrow

Data Protection Policy

and Privacy Notice

Policy last updated:	June 2024

CONTENTS

1. Definitions

EMMS International	A Charity Registered in Scotland No. SC032327
Data Controller	EMMS International
2018 Act	The Data Protection Act 2018
GDPR	The General Data Protection Regulation
Data Protection Officer	The EMMS International Director of Fundraising and Communications, Laura Brown, laura.brown@emms.org
Staff	Any employee, trustee, volunteer or consultant who has access to personal data held by EMMS International
Data Subject	The identified or identifiable living individual to whom personal data relates
Processing	Any operation performed on personal data, e.g. collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, restriction, destruction, erasure, or disclosure by transmission, dissemination or otherwise making available
Personal data	Information which relates to a living person (a 'data subject') who can be identified either from that data on its own (e.g. a name, identification number or IP address), or when taken together with other information which is likely to come into the possession of the data controller; any expression of opinion about the person and an indication of the intentions of the data controller or others, in respect of that person; does not include anonymised data.
Special category personal data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health, sex life and sexual orientation; Personal data held by EMMS International may be classed as special category personal data, either specifically or by implication, as it could be indicative of a person's religious beliefs.

2. Overview

This policy applies to all personal data for which EMMS International is responsible, all of which is stored electronically, except that on envelopes addressed to external

parties before postage. EMMS International needs to gather and use personal information about a variety of people, including employees, trustees, volunteers, supporters, event participants, programme partners and other contacts.

EMMS International takes the security and privacy of personal information seriously and is committed to processing data in accordance with its responsibilities under the 2018 Act and GDPR, which require all organisations that handle personal information to comply with a number of important principles regarding privacy and disclosure, and give people certain rights over the use of their data. The legislation regulates the way in which personal information about living individuals is collected, processed, stored or transferred.

3. Objective

The purpose of EMMS International's Data Protection Policy is to document the approach and provisions that EMMS International adheres to with regard to any personal data which EMMS International collects, processes, stores or transfers, and which others collect, process, store or transfer on behalf of EMMS International.

4. Scope

This Data Protection Policy applies to all personal information for which EMMS International is responsible, all of which is held electronically, except when ready to post. It applies regardless of where the information is held, and regardless of the ownership of the systems or infrastructure used for processing or storing the data.

EMMS International requires third party companies and individuals who work with EMMS International and who have access to personal information for which EMMS International is responsible to comply with the Data Protection Act 2018.

All staff are responsible for making sure that this policy is adhered to.

5. Data protection principles

EMMS International is committed to processing personal data in accordance with the undernoted key principles, as set out in the GDPR.

1. **Lawfulness, fairness and transparency** – personal data shall be 'processed lawfully, fairly and in a transparent manner in relation to individuals';

2. **Purpose limitation** – personal data shall 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';

3. **Data minimisation** – personal data shall be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed';

4. **Accuracy** – personal data shall be 'accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay';

5. **Storage limitation** – personal data shall 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; and 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';

6. **Integrity and confidentiality (security)** – personal data shall 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.

7. **Accountability** – EMMS International is responsible for complying with the GDPR and must be able to demonstrate compliance. 'The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 [the other data protection principles]'.

6. How personal data should be processed

Everyone who processes data on behalf of EMMS International has responsibility for ensuring that the data they collect, process, store and transfer is handled appropriately, in line with this policy and our Privacy Notice (an appendix to this policy).

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

The legal bases for processing personal data are that the processing is necessary for the purposes of EMMS International's legitimate interests; or to exercise the rights and obligations of EMMS International under employment law; or to meet a condition in Part 1, 2 or 3 of Schedule 1 of the Data Protection Act 2018 (in relation to processing of personal data relating to criminal convictions and offences or related security measures in a safeguarding context) .

Personal data held in all databases should be kept up to date. It should be securely and completely deleted when it is no longer needed for the purposes for which it is being processed. Unnecessary copies of personal data should not be made.

7. Privacy Notice *(Appendix 1)*

This policy including Privacy Notice is available on the EMMS International website.

8. Keeping personal data secure

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 data subject themselves or someone properly authorised to act on their behalf.

Access to folders on SharePoint containing electronic copies of personal information is limited to those staff who need access. Staff passwords to SharePoint should be kept secure, should be strong, changed regularly and not written down or shared with others.

EMMS International keeps hard copy personal information for up to 1 year.

Personal data should be encrypted or password-protected before being transferred electronically. Personal data should never be transferred outside the European Economic Area except in compliance with the law.

We will only share someone's personal data where we have a legal basis to do so, including for our legitimate interests within EMMS International.

9. Data Retention

EMMS International gathers personal information from individuals and external organisations and generates a wide range of personal data, most of which is recorded in electronic form, plus for a limited time on envelopes and letters for postage.

In certain circumstances, it is 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.

Data protection principles require information to be as up to date and accurate as possible. Therefore EMMS International operates a system for the timely and secure disposal of personal data that are no longer required.

10. Retention and disposal

Staff strive to keep records up to date, basing their decisions relating to the retention and disposal of data on the Data Retention Schedule in *Appendix 2*. The Data Retention Schedule provides guidance on the recommended and statutory maximum retention periods for specific types of documents and records.

11. Disposal

Electronic communications including email, Facebook pages, Twitter accounts and all information stored digitally should be reviewed and, if no longer required, closed and/or deleted 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 still exist in the electronic ether. Information will be deemed to be put beyond use if EMMS International is not able to use it in any way and cannot give any other organisation access to it.

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 removeable format);
- Sending the device to a specialist who will securely delete the data.

Hard copy documents which external parties may send to EMMS International and containing confidential or personal information is disposed of either by shredding or by using confidential waste bins or sacks. Such documentation may include names, address and financial details. Documents other than those containing confidential or personal information may be disposed of by recycling or binning.

12. How to deal with data security breaches

Any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data must be reported to the Data Protection Officer as soon as you become aware of the breach or potential breach. In cases of serious breach, where this is likely to result in a risk to the rights and freedoms of individuals, the Data Protection Officer must notify the UK Information Commissioner’s Office within 72 hours of EMMS International being made aware of said breach.

13. Data subject (Individual) rights

Data subjects (individuals) have certain rights under the GDPR:

- The right to be informed. This is provided in the EMMS International Privacy Notice
- The right to rectification of personal data
- The right to restrict processing of personal data (e.g. opt out of direct marketing)
- The right to object to processing of personal data
- The right not to be subject to automated decision-taking (e.g. profiling)
- The right to data portability
- The right to erasure of personal data (the ‘right to be forgotten’)
- The right to request any or all of the personal information held about them by a data controller. Such requests are known as Subject Access Requests (SARs) and are described more fully below.

Data should be erased when an individual revokes their consent, when the purpose for which the data was collected is complete, or when compelled by law.

All requests to have personal data corrected or erased should be passed to the Data Protection Officer, who is responsible for responding to them.

14. Subject access requests (SARs)

Data subjects can make a subject access request to find out what information is held about them. An SAR can be made verbally as well as in writing. Any such request received by EMMS International should be forwarded immediately to the Data Protection Officer, who will coordinate a response in writing within the necessary time limit (28 days or calendar month).

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

15. Contracts

If any processing of personal data is to be outsourced from EMMS International, for example to a mail fulfilment company, we will ensure that the mandatory processing provisions imposed by the GDPR are included in the agreement or contract.

16. Policy review

The Data Protection Officer is responsible for reviewing this policy annually and for updating staff on their data protection responsibilities and any risks relating to the processing of data.

APPENDIX 1 – Privacy Notice

Privacy Statement

EMMS International is an international healthcare charity working with overseas and Edinburgh partners to deliver improvements to aspects of healthcare.

It's good to share
At EMMS International we care about the relationships we have with our stakeholders (supporters, grant-givers, partners, staff and others), and we want you to feel that you can trust us to be diligent with your personal information. We will only communicate with you when we believe we have a legitimate interest to share information with you. This might include:

- Newsletters sharing information about our work,
- Information about events that may be of interest to you,
- Furthering our charitable mission (including fundraising and volunteer recruitment).

Our promise
We promise to keep your personal information secure. All third party organisations that we employ to support us in keeping in touch with you (e.g. mailing providers) will be contractually bound to hold your data only for the period required to conduct the activity, after which time your information will be returned to us or destroyed. All our suppliers are bound by UK data protection law (or equivalents of other countries) and you can be confident that we will ensure these suppliers are bona fide.

At any time you can ask us for a copy of the information we have about you using the contact details below. At any time, you can ask us to remove your data from our records, either because you no longer wish to hear from us or because the data we hold is no longer being used for the primary purpose for which it was given. We shall ensure that our third party partners remove your data from any records that they hold on our behalf.

Please tell us about any changes to your contact details, or preferences for method of contact so that we can keep our records accurate.

Your Information
We obtain personal information about you when you:

- sign up for more information,
- donate to EMMS International,
- participate in our fundraising activities or events,
- apply for one of our staff or volunteering roles,
- apply for funding.

You may give us your personal information indirectly through a donation on a third party fundraising site such as JustGiving. These third parties will ask you whether you are happy to be contacted by us. We will not use your information to contact you unless you give explicit permission on these sites (for example, ticking a box) or unless you have already given us permission directly to contact you.

We also gather general information about your use of our website, such as which pages you visit most often and which services, events or news items are of most interest to you. We may also track which pages you visit when you click on links in EMMS International's emails.

Our website uses cookies to provide functionality which enhances your experience. These include cookies used for analysis, social networking and the operation of the website.

We will only hold information on our database that helps us stay in contact with you or that we are required to hold for statutory reasons, e.g. for HMRC or OSCR. All stakeholder details are managed through our database which is held securely and managed in accordance with data protection legislation applicable in the UK. Personal information we hold may include:

- name, title, sex and date of birth;
- contact details including phone number or postal, social media or email addresses;
- information about your connection with EMMS International;
- family details and your relationships to other individuals or organisations;
- records of donations and Gift Aid status, where applicable (as required by HMRC);
- records of communications sent to you by EMMS International or from you to us;
- volunteering by you on behalf of EMMS International;
- information about you that you have shared with a member of our staff;
- media articles and legitimate information sources in the public domain;
- information on your engagement with EMMS International and our partners.

We will keep your information for the purposes for which it was given and will not keep it any longer than is required to fulfil these purposes, unless required to do so to fulfil statutory obligations (for example, to claim Gift Aid).
We periodically review whether we are using the most appropriate database for our purposes.

Your Rights
The Data Protection Act 2018 and General Data Protection Regulation gives you these rights:

The right to be informed of the information we are processing,
The right to access your information,
The right to rectification – if the information we hold about you is inaccurate**,**
The right to be forgotten,
The right to restrict processing,
The right to data portability – your right to request a copy of your personal information,
The right to object - your right to object to our processing of your personal information,
Rights about automated profiling - your right to object to automated processing of your information where this might lead to a decision with a significant effect on you. EMMS International does not conduct automated decision-making.

It's good to talk
If you'd like to talk to us about anything regarding privacy or fair processing in relation to your information please contact us by email at **info@emms.org** or by phone on **0131 313 3828.**

APPENDIX 2 – Data Retention Schedule

Data Retention Schedule

This schedule is provided as a guide to common types of data but is not exhaustive.

AREA	WHO IS COVERED?	MAXIMUM RETENTION PERIOD
HR	Current and former staff, contractors/ consultants, volunteers/interns and trustees	Duration of engagement & 6 years following cessation
	Unsuccessful job applicants, volunteers, contract staff	6 months after their last contact
Comms	Website enquiries – general public, contacts, current and potential supporters, other enquiries	12 months after their last contact
	Website – regular gift sign-ups, single gifts, G4L, event sign-ups	7 years after their last gift or last event (required for Gift Aid purposes)
	Email marketing – supporters, potential supporters, contacts, people registered on MailChimp	3 years of inactivity
	Photographs, videos, images, stories, case studies	Indefinite/archive
Events and Supporters	Prospective event participants	1 year or if request opt-out
	Church office-bearers (e.g. treasurer, Guild leader, elder)	Without limit while they are in this position (EMMS has legitimate interest), or until they request opt-out
	Supporters, people who have requested contact	6 years after their last contact
	Donors *(single gifts and regular gifts)*	7 years after their last gift
	Event participants	7 years from their last contact
Gift Processing	Supporters	7 years from their last contact
SEBs	SEB recipients	7 years from their report to EMMS on their grant, or 6 years after last contact, whichever is later
Programmes & Partners	Programme partners	7 years from the end of their last Project Agreement with EMMS or other funding from EMMS
Finance – Accounting	Staff and suppliers *(where these are individuals)*	7 years
Finance-payroll	Staff members	Duration of employment and 7 years after the end of the financial year in which they left