Society for Mucopolysaccharide Diseases
MPS House, Repton Place
White Lion Road, Amersham
Bucks, HP7 9LP

0345 389 9901
mps@mpssociety.org.uk
www.mpssociety.org.uk

Society for Mucopolysaccharide Diseases

Policy No. 1
DATA PROTECTION & PRIVACY POLICY

The Society appreciates the importance of demonstrating our adherence to the Data Protection Legislation by aiming to meet the expectations about the security and use of the personal information of all those on whom we hold such data – including but not restricted to members, supporters, beneficiaries, their respective families, volunteers and clinicians.

Our success is dependent on the quality of our reputation and the trust that all those involved or working for the Society have in the way we conduct ourselves. We are committed to do our very best to ensure the security of our website and the confidentiality of all the personal records we hold.

We only collect information that is voluntarily provided by these groups and visitors to our website, which only recognises a domain name and not email addresses. These will only be seen if an online form is completed.

The Society and Rare Disease Research Partners (RDRP) are joint data controllers for the processing of any personal information. This policy is applicable to both organisations. Personal information may be shared between these organisations on the basis of legitimate interest. Consent to share information in this way, may be withdrawn.

1. What is personal data?

Personal data is all information concerning or relating to any living individual. This includes personal data held in electronic records and also in manual records (eg: paper files, microfilm and other media). This applies to personal data held not only by the Society but also to personal data held or processed on its behalf by third parties.

Statistical reports and financial statements are not personal data as they cannot be related in any way to a living individual

2. Our commitment to each of the data protection principles is as follows:

a) We will process personal data in a lawful and fair way, so that those whose personal information is collected will have it used in a transparent way, with a clear explanation available for its use.

b) Our Annual Notification to the Information Commissioner's Office (ICO) will be checked to ensure that it represents the Society's current use of personal information. An audit will be carried out each year to achieve this. No data will be used for purposes other than those notified to the ICO. In the event that there is a requirement to change the usage of the data, all those about whom the data is held will be informed and given the opportunity to consent to this amendment.

Registered Charity No. 1143472. Registered as a Charity in Scotland No. SC041012
Registered as a Company limited by guarantee in England & Wales No. 7726882

c) Personal information will be adequate, relevant and not excessive for the purpose for which it is processed. Sufficient data will be obtained for clarity of recognition and to undertake the required administration of personal records. We will only hold the minimum of personal details required to achieve this.

d) Every effort will be made to keep records accurate and where necessary updated.

Updates of external personal records will be made within 28 days of change notification and internal HR records within 7 days or less depending on urgency.

e) In general all personal information records will be retained for 6 years, with any exceptions detailed in our Data Retention and Disposal Policy.

f) The Society gives data security the highest priority so that appropriate measures are in place to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

3. Good practice

a) Personal information will only be processed when absolutely necessary.
b) Individuals about whose information is obtained will be informed of the purpose for which their data is held.
c) Records will be kept of the categories of personal and sensitive data processed.
d) Individuals about whom data is held have the right of 'subject access' to see and / or amend any relevant errors or omissions.

4. Notification

The Society for Mucopolysaccharide Diseases and Rare Disease Research Partners have registered with the Information Commissioner (ICO) as Joint Data Controllers. This policy is applicable to both organisations. The notification will be reviewed annually.
Any breaches of this Policy will be dealt with according to the Employee Handbook, which may also be referred to the ICO for investigation.

All third parties are required to comply with this policy and also enter into a data confidentiality agreement. The Society may audit information held in respect of this.

5. GDPR definitions

Child means anyone under the age of 16. For those under 13, the consent of a parent/guardian is required.
Data subject refers to a living person about whose data is processed. This means identification by name, ID, address, online identifier or factors such as physical, psychological, genetic, mean, economic or social means.

Data subject consent may be given by a written or oral statement, having been properly informed, in a way which is informed, clear, specific, explicit and given freely.

Data breach refers to unauthorised disclosure, alteration, destruction or loss. All such breaches must be reported to the Society's Data Protection Officer who will assess whether the matter should be reported to the ICO. If this is the case, the ICO must be informed within 72 hours of the breach having been discovered. Whether this is required, will be assessed on the basis of the likelihood and severity of risk to the rights and freedoms of those affected. Similarly an internal decision will be taken on whether or not to inform the data subjects of the breach.

Special data categories (Previously known as sensitive data) refer to matters such as racial, ethnic origin, beliefs, political opinions, trade union membership, genetics, biometric identification, health, sexual orientation and sex life.

6. Data Protection Officer

Whilst all employees, temporary staff, volunteers and sub-contractors take individual responsibility for the personal information in their care, the Data Protection Officer takes over-arching management of this area.
He/ she reports to the Society's Board in respect of the development and implementation of the CRMS, as well as the day-to-day compliance with this policy.

This role also involves carrying out annual risk assessments to ensure on-going compliance and to identify areas where improvement is required. This person will oversee the requirement that data collected for one purpose is not subsequently used for another without appropriate consent.

Should any new technologies be incorporated, or any new data processing events be planned, then he / she must undertake a Privacy Impact Assessment. The ICO may also be contacted for advice in this instance.

The Data Protection Officer will ensure that appropriate controls are in place to ensure that the risk level is kept to an acceptance level.

Approval of all data collection forms and arrangements for deletion/ destruction according to the Society's Data Retention and Disposal Policy will also be the responsibility of the Data Protection Officer.

Training for both current and new staff will be determined by the Data Protection Officer.

The Data Protection Officer is the first point of contact for all employees who need guidance and must be informed immediately if there is any suspicion of a data breach.

7. Data subject awareness

All must be provided with the following information at time of data processing:

a) *Controller* – the identity of the organisation
b) *Purpose* – why the information is needed
c) *Storage period* - available on request
d) *Subject access* – how files can be made available for inspection and rectification

8. The rights of data subjects

a) The right to make subject access requests about their personal data which is held and to rectify any errors/omissions.

A data subject will be entitled to the following:

- A copy of his/her personal data
- The purpose of processing the data
- The organisations to whom the Society discloses the data
- A copy of recorded opinions about him/her, unless given in confidence

b) Any such information to be made available within one month of the original request. No charge can be made for this provision. The request must be made on the Society's form for this.

9. Consent

Consent for the processing of personal information must be:

a) informed
b) clear
c) specific
d) explicit
e) freely given

This can be provided in a written statement, or by affirmative action such as an online tick box offering an opt-in facility.

Consent can be withdrawn at any time.

Fundraising

The Society will provide an opt-out facility for supporters to stop postal mailings and an opt-in one to indicate their agreement to receive email communication.

Employees

They have been informed of their rights and obligations within the Employee Handbook.

10. Data security

All employees are personally responsible for keeping secure any of the Society's personal data.
Under no circumstances may it be disclosed to any third party without express authorisation, and that there is a confidentiality agreement in place.

Accessing and storing personal data

This must be stored in:

a) A locked room
b) In a locked cabinet or drawer
c) Encrypted

Computer screens and terminals must not be visible other than to the Society's staff.

No manual records may be removed without the written authorisation of a member of the MPS Senior Leadership Team or Data Protection Officer. The Manual Document(s) Removal Record will be completed at all stages.

Manual records must be shredded and disposed of as confidential waste. Any removable or portable computer media (eg USBs/hard drives) must be destroyed as per the Data Retention and Disposal Policy.

11. Disclosure of data

Employees must take steps to ensure that no personal data is disclosed to friends and family members. No disclosure to government bodies nor the Police may take place without the Data Protection Officer's agreement, having taken legal opinion and / or advice from the ICO.

Disclosure is permissible in certain circumstances such as:

a) In the interests of safeguarding national security
b) In the interests of crime prevention and detection
c) In the interests of discharging regulatory functions such as health & safety.
d) In the interests of serious harm occurring to a third party and

e) In the interests of protecting the vital interests of the data subject (ie in a life and death situation)
f) The Data Protection Officer is responsible for handling all such requests.

12. Data retention and disposal

This is determined on the basis of necessity and is documented in the Data Retention and Disposal Policy.

13. Future policy

Whilst we do not envisage any alterations to this Policy, should circumstances, legislation or technology change, the Society may need to update this. In such an event, any revisions will be posted on the website and staff will receive adequate briefing of any revisions.

14. Complaints

These should be addressed to the Data Protection Officer.

The Society for Mucopolysaccharide Diseases
MPS House
Repton Place
White Lion Road
Amersham
Bucks
HP7 9LP

In the event that a complaint is not dealt with satisfactorily, the matter can be raised to the ICO, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

15. Document owner

The data controller is the owner of this policy document and must ensure that it is periodically reviewed according to the review requirements contained herein.

The latest version of this policy document dated 08.04.2021 is available to all employees of the Society for Mucopolysaccharide Diseases on the corporate intranet.

This policy document was approved under the Society's policy approval process on a version controlled basis.

Name of GCEO: Bob Stevens Date: 08.04.2021

Document History			
Version	*Author*	*Date*	*Changes*
1.0	*Lesley*	*30.01.2021*	*First version*

Society for Mucopolysaccharide Diseases & Rare Disease Research Partners

REQUEST FORM FOR A COPY OF PERSONAL DATA

(Subject Access)

Section A

1. Full Name (Block letters) .....

2. Status (Delete as appropriate):

a. Current / former supporter;

b. Current staff / former staff member
(please specify department) ……

c. If neither supporter nor staff, what relationship have you had with the organisation when?

.....

3. Postal Address:

.....

.....

Email Address: .....

Records will be posted to you unless you ask specifically for an electronic (emailed) copy

4 Telephone number: .....

Section B

I, [*name*] wish to have access to data that the organisations have about me as outlined below:

Please specify from which organisation information is sought. *MPS* *RDRP* *Both* *Also please describe briefly the type of information sought and the relevant dates.*

Signed: ..... **Date:** .....

Please return this form to: