Royal Osteoporosis Society

Better bone health for everybody

Data Protection Policy

Policy implemented:	May 2018
Last reviewed:	-
Significant changes:	December 2024
Next review due:	December 2027

Data Protection Policy

1 Introduction and context

1.1 We're the Royal Osteoporosis Society – the UK's largest national charity dedicated to improving bone health and beating osteoporosis. And we're here for everyone. We equip people with practical information and support to take action on their bone health.

1.2 Working with healthcare professionals and policy-makers, we're influencing and shaping policy and practice at every level. We're driving the research and development of new treatments, to beat osteoporosis together.

1.3 During the course of its activities, the Charity will collect, store and process personal data about its employees, members, supporters, services users, suppliers and other third parties, and it recognises that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations. **Data processors** are obliged to comply with this policy when processing personal data on behalf of the Charity. All employees are required to comply with this policy, Data Protection Law and other relevant Charity policies. Any breach of this policy may result in disciplinary action.

1.4 The types of **personal data** that the Charity may be required to handle include information about current, past, prospective: beneficiaries, supporters, volunteers, suppliers and others that it communicates with. The Charity will also process personal data (which may be held on paper, electronically or otherwise) about its employees and it recognises the need to treat this data in an appropriate and lawful manner. Further details regarding how the Charity may handle the personal data it holds can be found in the relevant Privacy Policy. The Charity complies with the current Data Protection legislation in the United Kingdom, which includes the UK GDPR and the Data Protection Act 2018, plus any amendments or updates to these statutes. It also complies with other regulations relating to the use of personal data for marketing, including but not limited to, the Privacy & Electronic Communications Regulations 2003. We refer to this legislation as "Data Protection Law" in this policy.

1.5 The Charity has registered its data processing activities with the Information Commissioner's Office, registration reference: Z8568342 and acts as the **Data Controller**.

1.6 This policy is to be reviewed every 3 years to ensure it reflects current legislation and Charity practices. However, it may be updated at other times, as and when legislative changes occur.

1.7 Key terms used in this policy are defined in Appendix A.

2 Purpose and scope of the policy

2.1 The purpose of this policy is to outline how the Charity complies with Data Protection Law, and the rules that must be followed when handling personal data, such as how organisations are expected to keep data safe and the rights of individuals to whom the information relates.

2.2 This policy is aimed at employees, trustees, volunteers and individuals to whom the data relates, as well as third party suppliers. It refers to all data that identifies an individual whether stored electronically or in paper form within a Filing System.

2.3 All employees involved in dealing with information about individuals have a responsibility to follow this Data Protection Policy.

2.4 The Executive Team are accountable to the Board of Trustees for ensuring that this policy is followed and therefore complete spot checks from time to time. The occurrence of any data breaches is reported to the Board of Trustees and a monthly cross-functional group of Charity employees meet to review and monitor compliance. See section 12 for further details.

2.5 The Charity has appointed Paul Herbert as the trustee with particular responsibility for data protection.

2.6 All staff and volunteers have a role to play in our data protection compliance. Staff and volunteers are encouraged to ask questions and raise concerns with the Data Protection Lead or their line manager. This allows us to regularly review and strengthen the data protection measures that we have in place.

3 Data Protection Lead

3.1 The Charity has named Data Protection Lead who reports to the Board of Trustees on a quarterly basis.

3.2 The role of the named Data Protection Lead is:

3.2.1 To inform and advise the organisation and its employees about their obligations to comply with Data Protection Law.

3.2.2 To monitor compliance with Data Protection Law, including managing internal data protection activities, advising on data protection impact assessments and ensuring all staff are trained in the basic principles of Data Protection.

3.2.3 To be the first point of contact for supervisory authorities and for individuals whose data is processed, for example, employees and supporters.

3.3 The named Data Protection Lead is the People & Governance Advisor and if you have any questions or complaints related to this policy the named Data Protection Lead can be contacted:

Data Protection Lead
Royal Osteoporosis Society
St James House
The Square
Lower Bristol Road
Bath BA2 3BH

Telephone: 01761 473115 or General Enquiries 01761 473287
Email: dataprotection@theros.org.uk

4 Compliance measures

4.1.1 The Charity helps to ensure compliance with data protection law using the measures outlined at paragraphs 5 to 16 below.

5 Training

5.1 The Charity ensures that all employees and volunteers processing data on its behalf receive annual Data Protection training and regular reminders regarding the rights of individuals, as set out below. The Individual Rights section (paragraph 10 below) outlines the rights of individuals to access the data held about them.

5.2 Further information related to privacy can be found in our Privacy Policy, available on the website.

5.3 The Data Protection Lead attends regular external training which is appropriate to their role as the senior individual who leads on the Charity's data protection compliance.

5.4 Other teams and departments are given data protection training which is specific to their role or function.

6 Policies and guidance

6.1 All staff and volunteers at the Charity are required to comply with the following documents:

6.1.1 Data Protection Policy: Practical Guidance for Staff;

6.1.2 Information Security Assurance Policy;

6.1.3 Privacy Policy; and

6.1.4 Call Recording Policy.

6.2 The Data Protection Lead is responsible for implementing the:

6.2.1 Data Breach Policy and Procedure;

6.2.2 Information and Records Retention Policy;

6.2.3 Appropriate Policy Document for special category personal data.

7 Documentation

7.1 Documenting how we comply with data protection law is a key part of our compliance. In addition to the documents listed at section 0 above we:

7.1.1 maintain a record of how we use personal data as required under Article 30 of the UK GDPR. The Data Protection Lead is responsible for maintaining this record;

7.1.2 document our lawful bases for using personal data through our privacy notices;

7.1.3 keep a record of our legitimate interests assessments;

7.1.4 carry out risk assessments and when required a Data Protection Impact Assessment;

7.1.5 retain records of any consents obtained to use personal data by storage of such consents on the Charity's database, also known as CRM (Customer Relationship Management software).

7.1.6 maintain a register of any data breaches. The Data Protection Lead is responsible for completing this. All staff understand that they must inform the Data Protection Lead of any suspected breach so that the register can be kept up to date;

7.1.7 record when staff complete data protection training to ensure that all staff have received the appropriate level of training; and

7.1.8 maintain an Appropriate Policy Document regarding our processing of special category personal data and criminal offence data as required by the DPA 2018.

8 Privacy notices

8.1 The Charity has privacy notices, which are published on the Charity's website.

8.2 In addition, the Charity explains how personal data will be used on a case by case basis as appropriate. For example, forms that are used to collect personal data will include a brief description of how and why it will be used, and cross refer to the applicable privacy notice.

9 Data protection by design and default

9.1 The Charity has built the data protection principles into its practices by implementing appropriate technical and organisation measures. This is known as data protection by design.

9.2 We also ensure that we only use the minimum amount of personal data to achieve our purposes - known as data protection by default.

9.3 More specifically we do the following:

9.3.1 at the start of any new project, or new activity, which involves using personal data (e.g. working with a new external activity provider, implementing new software or hardware) the Data Protection Lead considers how we will comply with the data protection principles;

9.3.2 we make it clear on any data collection forms what personal data must be provided and what is optional;

9.3.3 we proactively consider data protection risks and adopt appropriate measures to protect personal data (e.g. encryption, physical security);

9.3.4 our external facing documents (e.g. privacy notices) are accessible and age appropriate;

9.3.5 before we share personal data externally we check that we have a lawful basis and that the sharing is fair;

9.3.6 we regularly review the measures which are in place to ensure that they are still appropriate;

9.3.7 we have developed a culture where staff understand the importance of data protection; and

9.3.8 if there has been a problem, or a "near miss", we will look at what has happened to improve our practices, for example, by providing additional staff training and awareness.

9.4 The Data Protection Lead determines whether a Data Protection Impact Assessment is required before the Charity begins any new type of processing activity. For example, before the Charity introduces new software to store records.

10 Individuals' rights

10.1 We are committed to allowing individuals to exercise their rights under the UK GDPR. These rights are as follows:

10.1.1 right of access (i.e. making a subject access request);

10.1.2 right to rectification;

10.1.3 right to erasure;

10.1.4 right to restriction;

10.1.5 right to data portability; and

10.1.6 right to object; and

10.1.7 rights in relation to automated decision-making and profiling.

10.2 Staff are trained to recognise when an individual is exercising a right under the UK GDPR and to pass this immediately to the Data Protection Lead.

10.3 The Charity keeps a log of all requests to exercise rights with the applicable deadline for our response. This log is maintained by the Data Protection Lead.

10.4 To ensure that we meet our obligations the Data Protection Lead co-ordinates our response to all requests. The Data Protection Lead has knowledge of how to respond to individuals' rights. The Data Protection Lead will involve other members of staff, as appropriate, in formulating the Charity's response.

10.5 Consideration is given to at least the following issues when responding to rights requests:

10.5.1 the importance of responding within the statutory timeframe, usually one calendar month (but this can be extended by up to two months for complex requests);

10.5.2 whether further engagement with the requester is needed, e.g. to ask for ID or to seek clarification of their request;

10.5.3 the exemptions under the Data Protection Act 2018;

10.5.4 the provision of supplementary information (e.g. sources and purposes) under a subject access request;

10.6 whether the request can be refused, or a reasonable fee charged, because it is manifestly unfounded or excessive; and

10.6.1 how to securely send our response to the requester.

11 Information security

11.1 The Charity has put in place technical and organisational measures to ensure the confidentiality, availability and integrity of personal data. The Data Protection Lead is responsible for determining the appropriate organisational measures, for example, staff training and guidance.

11.2 The Finance and IT Director leads on the technical side of our information security, for example, network security. The Charity follows guidance from the National Cyber Security Centre and keeps up to date with the latest cyber security news and alerts.

11.3 The Charity has implemented an Information Security Assurance Policy for staff.

11.4 We appreciate that prompt action is vital when handling information security incidents. Staff are trained to report any suspicions or concerns regarding potential personal data breaches to the Data Protection Lead immediately.

11.5 The Data Protection Lead will carry out an initial investigation and determine if the incident constitutes a personal data breach. If so, the procedure outlined in the Data Breach Policy and Procedure will be followed.

11.6 Security procedures include:

11.6.1 Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal Data is always considered confidential.)

11.6.2 Methods of disposal. Confidential waste bins and shredding facilities are provided at the Head Office.

11.6.3 Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they use the Windows lock screen function when leaving their desk.

12 Data Breaches

12.1 Should there be a breach of Data Protection Law, including the Data Protection Principles, this would be described as a **Data Breach**. There is a requirement to report certain types of data breaches to the Information Commissioner's Office, within 72 hours of first becoming aware. There is also a requirement to notify Individuals about breaches in certain circumstances.

12.2 Reporting of a data breach to the regulator is considered on a case-by-case basis, with all breaches following the Charity's Data Breach Reporting Process overseen by the Data Protection Lead. This ensures that, where appropriate, the Information Commissioner's Office, and the individuals concerned are notified in line with the requirements.

12.3 All Data Breaches are taken seriously and must be reported to the named Data Protection Lead at the earliest opportunity. All data breaches are reported on a quarterly basis to the Board of Trustees, and actions are taken to ensure that any weaknesses in security are quickly identified and resolved. Reporting and identification of all breaches – including any "near misses" enable us to assess weaknesses in our processes and systems, and to plug any gaps, so it is important we're aware of all possible breaches.

13 Processors

13.1 The Charity has procedures in place to check that the organisations acting as our processors are complying with the UK GDPR. The Data Protection Lead the lead of any such contracts are responsible for implementing these procedures.

13.2 The Charity has contracts in place with our processors which include the specific terms required by the UK GDPR. Legal advice is sought as required regarding these contracts.

13.3 Staff are trained to speak to the Data Protection Lead if they need to share information with an organisation which may act as the Charity's processor so that the Data Protection Lead can check that the appropriate measures are in place.

14 International transfers

14.1 The Charity maintains a record of when it transfers personal data outside of the UK and what adequacy decision, safeguard or derogation is relied on under the UK GDPR. The Data Protection Lead is responsible for maintaining this record.

14.2 Staff are trained to speak to the Data Protection Lead before transferring personal data outside of the UK.

15 Data Protection Fee

15.1.1 The Charity has procedures in place to ensure that the data protection fee is paid to the Information Commissioner's Office.

15.1.2 The Data Protection Lead is responsible for ensuring the fee is paid on time.

16 Our complaints procedure

16.1 If an Individual is not satisfied by the Charity's actions in relation to this policy, they can seek recourse through the Charity's internal complaints and appeals procedure, the Information Commissioner, or the courts.

16.2 The Charity's Data Protection Lead will deal with any written complaints concerning the way a request has been handled and what information has been disclosed. By email at dataprotection@theros.org.uk, or post to the Royal Osteoporosis Society, St James House, The Square, Lower Bristol Road, Bath, BA2 3BH.

16.3 If an Individual remains dissatisfied, they have the right to refer the matter to the Information Commissioner.

The Information Commissioner can be contacted at:

Information Commissioner's Office (Head Office)
Wycliffe House
Water Lane
Wilmslow
Cheshire, SK9 5AF
Telephone: 0303 123 1113 / 01625 545 745
https://ico.org.uk/global/contact-us

16.4 The Information Commissioner's Office can also provide further information in relation to the rights of Individuals.

16.5 Any Charity employee or volunteer with queries regarding the content of this policy should contact the Data Protection Lead.

17 Monitoring and review

17.1 The Data Protection Lead will ensure that the content and implementation of the procedures set out in this policy are reviewed regularly.

Appendix A: Definitions

Personal data: information which identifies a living individual, is biographical or which has the individual as its focus and which affects the privacy of that individual, either in a personal or professional capacity. Any expression of opinion about the individual or any indication of the intentions of any person in respect of the individual will be personal data.

Provided the information in question can be linked to an identifiable individual, the following are likely to be examples of personal data:

- an individual's salary
- information about an individual's family life or personal circumstances,
- employment or personal circumstances, any opinion about an individual's state of mind

The following are examples of information, which will not normally be personal data:

- mere reference to a person's name, where the name is not associated with any other personal information
- incidental reference in the minutes of a business meeting of an individual's attendance at that meeting in an official capacity
- where an individual's name appears on a document or email indicating only that it has been sent or copied to that particular individual
- the content of that document or email does not amount to personal data about the individual unless there is other information about the individual in it.

Special categories of data: an individual's racial or ethnic origin, political opinions, religious beliefs, physical or mental health, sexual orientation, criminal record and membership of a trade union. This information requires additional protection under the UK GDPR.

Data Subject: the individual that is identifiable from the information.

Data Controller: determines the purposes and means of processing personal data.

Data Processor: is responsible for processing personal data on behalf of a controller.

Filing System: any structured set of personal data which are accessible according to specified criteria (such as hard copy files relating to individuals e.g. personnel files)

Data Breach: is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. A breach is therefore more than just losing personal data.