Royal Osteoporosis Society

Better bone health for everybody

Data Protection Policy

Juliette Morgan, Data Protection Officer
Authors: Juliette Morgan, Head of Corporate Governance, Sarah Whybrew, Corporate Governance Manager
Audience: General public, employees and volunteers
Implementation date: 25 May 2018
Review date: February 2021
Updated to Royal Osteoporosis Society on 5 February 2019

Contents

1. Introduction and context

The Royal Osteoporosis Society (hereafter known as 'the Charity') is an incorporated charity, whose objectives are to relieve sickness and to promote and advance medical knowledge, with particular reference to all aspects of osteoporosis and all similar and related conditions and to undertake research in relation thereto, and to publish the useful results of such research. The Charity does this by raising money to fund scientific research on treatments and to provide services and support to people affected by the disease.

During the course of our activities, the Charity will collect, store and process personal data about its employees, customers, 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 contractually bound to comply with this policy and the current Data Protection legislation and other relevant Charity policies. Any breach of this policy may result in disciplinary action.

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 its privacy policy. The Charity complies with the current Data Protection legislation in the United Kingdom, and will comply with the European Union General Data Protection Regulation, effective 25th May 2018 onwards. 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.

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

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.

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

2. Purpose and scope of the policy

The purpose of this policy is to outline how the Charity complies with the current Data Protection legislation, 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.

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.

All employees involved in data processing have a responsibility to follow the Data Protection Policy, Data Retention Policy and Subject Access Request Policy.

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 to ensure the policy is being followed. The occurrence of any data breaches is reported to the Board of Trustees and a quarterly cross-functional group of Charity representatives meet to review and monitor compliance. See section 4.8 for further details.

Any breaches of this policy will be taken seriously and disciplinary procedures may be followed at the discretion of the Head of HR and the employee's Line Manager.

3. Data Protection Principles

3.1 What is the current Data Protection legislation?

From 25th May 2018 the Data Protection legislation enforced in the United Kingdom is the European General Data Protection Regulation (GDPR) which will sit alongside the UK Data Protection Act 2018. The UK Data Protection Act 2018 provides further detail concerning the application of the GDPR in the UK.

The rights of the individual with regards to data protection have been strengthened and the updated legislation overrides the Data Protection Act 1998. The GDPR has been adopted by those countries in the European Union ("EU") and applies to any data processing activities carried out by organisations operating within the EU or by organisations outside the EU that offer goods or services to individuals within the EU.

The Regulation states that anyone who processes personal information must comply with the following six principles, which make sure that personal information is:

- Fairly and lawfully processed, in a transparent manner. This means an individual's personal data should be handled in a way they would reasonably expect and for defined purposes.
- Processed for specific, explicit and legitimate purposes. This means individuals need to be told about why their personal data has been collected and what will be done with it.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. This means that personal data held about an individual should be sufficient for the purpose it held for and ensuring that no more information is held or used than required for that purpose.
- Accurate and up to date. This means systems and processes must be in place to ensure the accuracy of any personal data and reasonable steps should be taken to ensure that inaccurate data is rectified
- Not kept for longer than is necessary. This means personal data should be retained no longer than is necessary for the purpose it is obtained for.
- Secure. This means appropriate security must be in place to prevent the personal data held being accidentally or deliberately compromised.

There is a requirement for the **Data Controller** to demonstrate compliance with these principles. This is known as the principle of accountability.

4. How does the Charity follow the Data Protection Principles?

4.1. Fair and lawful processing

In order to ensure that personal data is fairly and lawfully processed the Charity keeps a record of the legal grounds for processing for all personal data we collect or receive. Most processing carried out by the Charity is covered by one of the following legal grounds for processing:

- the individual has consented to the processing
- the processing is necessary for the performance of a contract with the individual in question
- the processing is necessary for compliance with a legal obligation
- the processing is necessary to protect the vital interests of the data subject or another person
- the processing is necessary for the performance of a task in the public interest or in the exercise of official authority vested in ROS
- the processing is necessary for the purposes of ROS or a third party's Legitimate Interests

We request and record consent for personal data collected in relation to marketing and fundraising materials, except in the case of: Members, where we are fulfilling a contractual requirement to send communications concerning the work of the Charity; Major Donors, prospective Major Donors, and prospective Members, where we rely on **Legitimate Interest** to process Personal Data. In all cases where Legitimate Interest is relied upon as the legal basis for processing personal data, a balancing exercise is completed to review whether the individual's rights and freedoms override the legitimate interests of the Charity or third party. All balancing exercises must be approved by the Charity's Data Protection Officer before Legitimate Interest is relied upon.

Full details of the legal grounds for processing personal data and when they are used by the Charity can be found in the Charity's privacy policy.

4.2. Processed for specific, explicit and legitimate purposes

The Charity has a privacy policy which explains why personal data is collected and what will be done with it.

4.3. Adequate, relevant and limited to what is necessary

The Charity considers what information is relevant and that any personal data collected is limited to what is necessary in relation to the purposes for which it is processed.

4.4. Kept accurate and up to date

The Charity ensures that it has systems and processes in place to ensure the accuracy of any personal data and that reasonable steps are taken to ensure that inaccurate data is rectified.

4.5. Not kept for longer than is necessary

The Charity has a Data Retention Policy (see section 5 below) which ensures that the data it holds is not retained for longer than necessary. Data which is no longer required, as outlined in section 5, is securely destroyed.

4.6. Processed in line with the individuals' rights

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 Subject Access Policy (section 7 below) outlines the rights of individuals to access the data held about them.

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

4.7. Security

The Charity ensures that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

The Charity has in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. The Charity will only transfer personal data to a Data Processor if they agree to comply with those procedures and policies, or if they put in place adequate measures.

The Charity maintains data security by protecting the confidentiality, integrity and availability (for authorised purposes) of the personal data, defined as follows:

(a) Confidentiality means that only people who are authorised to use the data can access it.
(b) Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
(c) Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the Charity's central computer system instead of individual PCs.

Security procedures include:
(a) Entry controls. Any stranger seen in entry-controlled areas should be reported.

(b) 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.)
(c) Methods of disposal. Confidential waste bins are provided at the Head Office and shredding facilities are provided for all employees working remotely to ensure that all paper documents can be shredded. Digital storage devices are physically destroyed by our I.T. contractor when they are no longer required.
(d) 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.
(e) Encryption. Most of the data held by the Charity is encrypted using Microsoft systems, and emails and memory sticks are encrypted to ensure protection of data transferred outside of the Charity.

Our Information Security Policies provide further detail of how data will be held securely.

We work with our third-party suppliers to ensure that they also comply with current Data Protection legislation, and ensure that any data transferred to suppliers based in the EU or outside of the EU is also protected. Data Processors also have a responsibility to comply with the requirements of the Data Protection Act and the GDPR, and at the point of appointing a third-party supplier, their ability to comply and ensure the security and protection of any personal data passed to them will be reviewed and documented by the Data Protection Officer.

4.8. What happens if these principles are not adhered to?

Should there be a breach of the Data Protection legislation, 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 relevant supervisory authority, the Information Commissioner's Office, within 72 hours of first becoming aware. There is also a requirement to notify Data Subjects about breaches in certain circumstances.

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

All Data Breaches are taken seriously and must be reported to the Data Protection Officer 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.

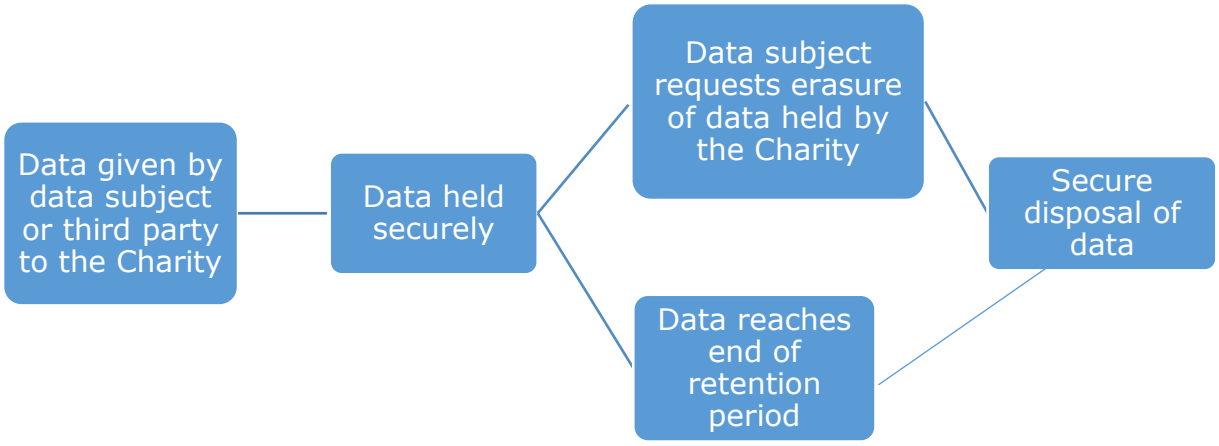
5. Data Retention Policy

5.1. Purpose of the policy

In order to ensure that personal data held by the Charity is not kept for longer than necessary, the below Data Retention Policy (at Appendix B) outlines how the Charity will meet the requirements of the current legislation and follow best practice in this area.

This policy outlines how the personal data held by the Charity will be kept secure, how long it will hold onto it and how it will ensure it is securely destroyed at the end of the retention period. This relates to data held internally within the organisation, and also data held externally with third party suppliers. Appendix B refers not only to personal data but also organisational data. In addition, there is consideration of an individual's right to request erasure of their personal data (also known as the right to be forgotten) and the implications for data retention.

Diagram 1: The simplified journey of data from entry to exit



5.2. Right to Erasure (Right to be forgotten)

There may be circumstances in which the data is not retained for the period set out in Appendix B. For example, Data Subjects now have the "right to erasure", otherwise known as the "right to be forgotten", which means that they can request the erasure of personal data in certain circumstances, including:

- where the personal data are no longer necessary in relation to the purposes for which they were collected or processed;
- where the data subject withdraws consent and the Charity relied on consent as a ground for processing and there is no other legal ground for processing;
- where the data subject objects to the processing and there are no overriding legitimate grounds for the processing; or
- where the personal data has been unlawfully processed.

The Charity can refuse to comply with a request for erasure if the data is being processed for the following reasons:

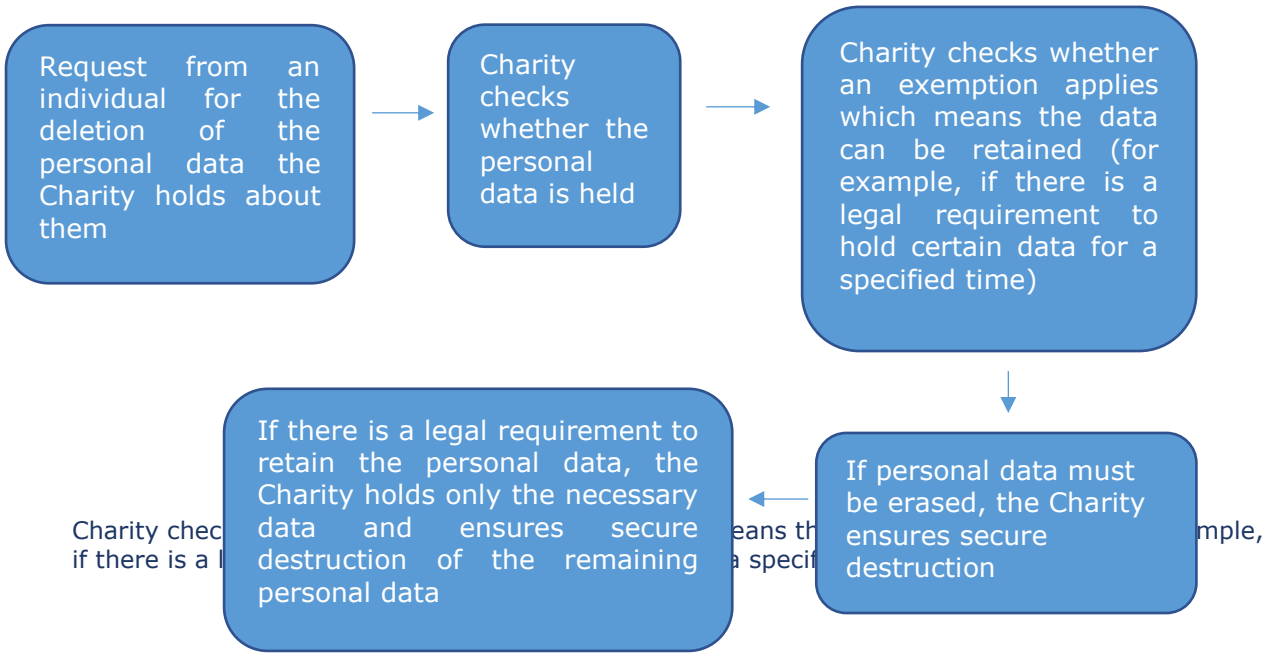
- the processing is necessary for exercising the right of freedom of expression and information;

- the processing is necessary to comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
- the processing is necessary for public health purposes in the public interest;
- the processing is necessary for archiving purposes in the public interest, scientific research, historical research or statistical purposes; or
- the processing is necessary for the exercise or defence of legal claims.

For example, the Charity will continue to hold an individual's data in relation to a donation that was made during the previous 7 years (even if they request the erasure of this information) because this is a legal requirement.

The following diagram demonstrates the process that is followed on receipt of a request for erasure.

Diagram 2: Process following request for erasure



An audit trail of consent and any requests in line with the individual's rights, related to the processing of data is retained and recorded as evidence of consent and is to be stored on the Charity's database, also known as Customer Relationship Manager (CRM).

An individual can request their data is deleted by using the contact details in Section 7.

5.3. Disposal of Data

Once the data has been retained for the periods outlined in Appendix B, or in the event the Charity is required to comply with a request for erasure the Charity will ensure that all data is destroyed securely as outlined in Appendix C.

5.4. Implementation of the policy

This policy is to be circulated to all staff, trustees and volunteers as part of their induction, and will be referred to as part of the annual Data Protection refresher training. In order to demonstrate that the policy has been read and understood the appropriate policy agreement form will be signed, and compliance with this policy, and others, will be monitored as part of regular supervision and appraisals.

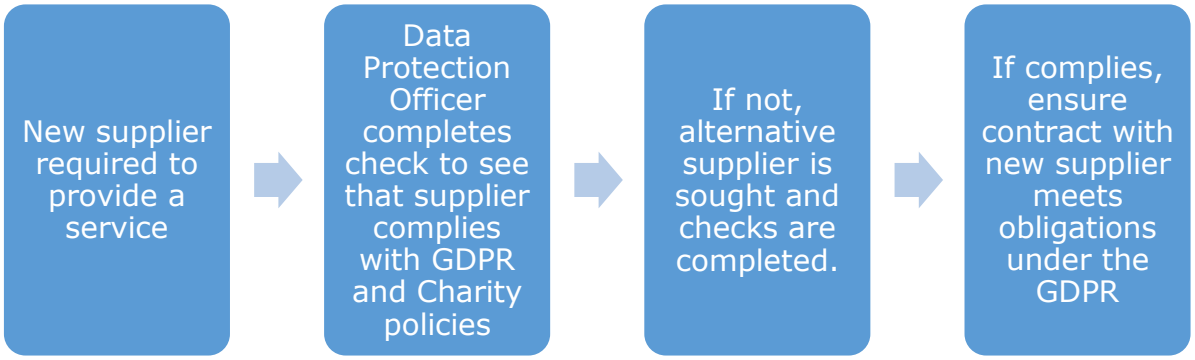
Controls will be put in place to ensure that the Charity complies with the policy and the requirements regarding the retentions and destruction of personal data as outlined in Appendix B and C. In particular, the relevant Heads of Development will liaise regularly with their teams to ensure compliance and will complete data protection audits and spot checks as required. In addition, there will continue to be quarterly compliance meetings for a group of Charity representatives from across the organisation to monitor the implementation of the retention schedule.

Any concerns identified will be reported to the Data Protection Officer to ensure that any identified risks are included on the Risk Register and controls are put in place to mitigate these risks.

5.5. Data Retention and Third-Party Suppliers

At the point of contracting a third-party supplier to carry out a service on behalf of the Charity, the Charity will ensure that information is only retained for as long as necessary to provide the specified service, and only the appropriate data is shared.

Diagram 3: The process followed when appointing a third-party supplier



For example, where the Charity contracts third-party suppliers to securely destroy confidential papers and computer hardware, secure disposal will be discussed with the supplier at the point of agreeing a contract. Where appropriate, further measures to ensure compliance will follow, such as requesting a certificate of destruction to evidence that the data has been securely destroyed.

In addition, where suppliers act as Data Processors on behalf of the Charity, the above procedures will be followed to ensure that any data or communication preferences that are updated are passed onto any other relevant Data Processors as well.

A review will be completed with suppliers on at least an annual basis to review their compliance, assessing how they continue to meet the requirements.

5.6. Introduction to the Data Retention and Disposal Schedule

The Data Retention and Disposal Schedule (Appendix B) has been created to ensure there is a clear framework in place for all those involved in managing information across the Charity. The information has been categorised to allow for clear decision making around how long specific documents or types of data should be retained for. The length of retention considers the legal requirements, good practice guidelines, and the benefits of the organisation retaining such information.

6. Data Subject Rights

Rights for individuals have been strengthened under the GDPR and are as follows:

- The right to be informed about the Charity's data collection and data processing activities
- The right of access to their own personal data
- The right to rectification of their personal data in certain circumstances
- The right to erasure of their personal data (also known as the right to be forgotten)
- The right to restrict processing of their personal data in certain circumstances
- The right to data portability i.e., the right to receive a copy of their personal data or transfer the personal data to another data controller
- The right to object to the processing of their personal data
- The right not to be subject to automated decision making and profiling.

Further information concerning data subject rights, how to go about actioning those rights and any exemptions, are available as part of our privacy summary on the Charity's website, *www.theros.org.uk*.

7. Subject Access Request Policy

7.1. What is a Subject Access Request (SAR)?

A subject access request is a written request for personal information (known as personal data) held about a Data Subject by the Charity. A Data Subject has the right to access to your personal data and also to obtain the following:

- confirmation that their data is being processed;
- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom the personal data is disclosed;
- the envisaged period for which the personal data will be stored (or the criteria used to determine that period);
- the existence of the right to request rectification or erasure, to object to or to request the restriction of the processing;

- the right to lodge a complaint with the Information Commissioner's Office;
- any available information as to the source of the personal data; and
- the existence of any automated decision-making, including profiling.

7.2. How does a Data Subject make a subject access request?

In order to make a subject access request a Data Subject can contact the Charity via telephone: 01761 473 257

Email: dataprotection@theros.org.uk

Or by completing the form on our website: www.theros.org.uk

To process a subject access request, the Charity requires Data Subjects to complete the form found in Appendix E, or a letter or email outlining the information being requested and any specific time periods the request relates to.

See Appendix D for details of the process for dealing with subject access requests. Employees should ensure that any subject access requests they receive are forwarded to the Data Protection Officer so that they can be dealt with.

7.3. Will we charge a fee?

No, not usually. There is no fee to make a subject access request, however if the request is manifestly unfounded or excessive the Charity may use its discretion to charge a reasonable fee. If this is the case the Data Subject will promptly be contacted.

7.4. What is the timeframe for responding to subject access requests?

The Charity has one month (starting from when it has received all the information necessary to identify the Data Subject and fulfil the request) to provide the information or explanation about why it is unable to provide the information. This can be extended in certain circumstances, such as where the request is particularly complex. The Charity will update Data Subjects within the initial one month period if this is the case.

7.5. Are there any grounds we can rely on for not complying with a subject access request?

We do not have to comply with a request if it is manifestly unfounded or excessive, in particular, because of their repetitive nature.

There are a number of legal exemptions which may apply and mean that there is no requirement to disclose personal data to a Data Subject. We may seek legal advice if we consider that they might apply. Exemptions include where the personal data attracts legal professional privilege or constitutes the personal data of a third party.

7.6. What if the personal data we hold is inaccurate?

If we agree that the information is inaccurate, we will correct it. We may add a supplementary statement to the personal data to rectify any inaccuracies. Where practicable, we may also destroy the inaccurate information. If the information in question has been passed to a third party for processing we will inform them of the correction where possible.

7.7. What if a Data Subject wants the Royal Osteoporosis Society to stop processing its data?

In certain circumstances Data Subject has the right to request that the processing of their personal data is restricted. However, the Charity may refuse to comply with such a request, for example, where the processing is required for the defence of legal claims.

If a Data Subject wishes to change their communication preferences or restrict further processing of their data, they should contact the Charity using the Data Protection Officer's contact details below with their full name. If they contact the Charity directly it can also confirm what processing has been stopped.

If a Data Subject does not wish to be contacted by the Charity or any other charity they can also sign up to the Fundraising Preference Service via

https://public.fundraisingpreference.org.uk/

If the Data Subject signs up to the Fundraising Preference Service the Charity will not contact them to confirm that communication has been stopped.

8. The role of the Data Protection Officer

The Charity has appointed a Data Protection Officer who reports to the Board of Trustees on a quarterly basis.

The role of the Data Protection Officer is:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments; training staff and conducting internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed, for example, employees and supporters.

The Data Protection Officer is the Head of Corporate Governance and if you have any questions or complaints related to this policy the Data Protection Officer can be contacted:

Telephone: 01761 473251 or via General Enquiries 01761 473257.

Email: dataprotection@theros.org.uk

Address: Data Protection Officer
Royal Osteoporosis Society
FREEPOST RTJH-ERRL-ZEBK
Manor Farm
Skinners Hill
Camerton
Bath
BA2 0PJ

9. Our complaints procedure

If a Data Subject 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.

The Charity's appointed Data Protection Officer, the Head of Corporate Governance, 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, Manor Farm, Skinners Hill, Camerton, Bath, BA2 0PJ.

If a Data Subject 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/

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

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

10. Accountability Framework

All employees involved in data processing have a responsibility to follow the Data Protection Policy, Data Retention Policy and Subject Access Request Policy.

The Executive Team are accountable to the Board of Trustees for ensuring that this policy is followed and may therefore complete spot checks from time to time to ensure the policy is being followed.

Any breaches of this policy will be taken seriously and disciplinary procedures may be followed at the discretion of the Head of HR.

11. Related policies

- Information Security Assurance Policy
- Complaints Policy
- Privacy Policy
- Call Recording Policy

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 (previously known as sensitive information): 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 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)

Legitimate Interests: is one of the six lawful bases for processing personal data. It can be relied upon when the processing is necessary for an organisation's legitimate interest or the legitimate interest of a third party unless there is good

reason to protect the individual's personal data which overrides those legitimate interests. It is most likely to be applicable when the Charity uses people's data in ways they would reasonably expect and which have minimal privacy impact.

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.

Prospective Members: individuals who have contacted the Charity to request information, and are informed about membership subscription entitling them to exclusive membership benefits.

Prospective Major Donors: high profile individuals who are potential Patrons of the Charity, attendees of high profile events, or through their public profile or role as a trustee of a charitable trust are perceived to have an interest in supporting the work of the Charity.

Major Donors: individuals who are Patrons of the Charity, and/or have previously attended high profile events organised by the Charity and have recently made a donation to the Charity.

Members: individuals who have paid a subscription to receive exclusive membership benefits.

Further information is also available from the Information Commissioner's Office: *www.ico.org.uk*

Appendix B: Data Retention and Disposal Schedule

*these fields are considered discretionary, and the retention period can be extended where there is an appropriate justification agreed by the Data Protection Officer.

Type of Data	Retention Period	Reason for length of period	Accountable Person
Financial			
Accounting records related to income and expenditure	6 years from the end of the financial year the transaction was made.	Companies Act/Charities Act/HMRC requirements	Finance Director
Gift Aid declarations	To be retained whilst in use and destroyed 6 years after it is no longer required.	HM Revenue & Customs	Finance Director
Legacies - Pecuniary Paper Files	5 years following receipt of legacy payment and file closure	Data Protection Act	Legacy Manager
Legacies - Residuary Paper Files	10 years following receipt of legacy payment and file closure	Data Protection Act	Legacy Manager
Legacies - Correspondence and history of events	Permanently*	Organisational Benefit and to bequest future associated legacies	Legacy Manager
Legacies - Executor contact and payment details	Permanently*	Organisational Benefit and to bequest future associated legacies	Legacy Manager
Successful quotations for capital expenditure	Permanently*	Commercial considerations	Finance Director
Invoice for a capital item	To be retained whilst the capital item is still in use and destroyed 6 years after the capital item has been removed from the fixed asset.	Companies Act/Charities Act/HMRC requirements	Finance Director

Contract with customers, suppliers or agents, licensing agreements, rental/ hire purchase agreements, indemnities and guarantees and other agreements or contracts	6 years following the end of the contract or the end of the accounting year whichever is later.	Limitations Act 1980	Finance Director
Payroll Documentation, including Statutory Sick Pay records and calculations	6 years plus current year	Taxes Management Act/ Pensions Act/Companies Act/Charities Act	Finance Director
PCI Documentation related to card payments	6 years from the end of the financial year the transaction was made.	The Payment Card Industry Data Security Standard (PCI DSS)	Finance Director
Credit reference information	1 year	Commercial considerations	Finance Director
Pension Information related to employees	6 years after employment ceases	Data Protection Act	Finance Director
Annual Accounts and Annual Report	Permanently	Data Protection Act	Finance Director
Balance sheet items, e.g. current assets and liabilities	Retained whilst current and then destroyed 6 years from the end of the financial year of the last transaction	Companies Act, Charities Act, HMRC requirements	Finance Director
Investment Reports	6 years from the end of the financial year after investment ceases.	Companies Act, Charities Act, Commercial	Finance Director
Fixed Assets Register	Permanently	Companies Act, Charities Act, Commercial	Finance Director
Employee/Personnel Records			
Personnel files, including training records, supervision notes, appraisals, sickness certificates, and all other documentation related to employment. This exclude any disciplinary records.	6 years after employment ceases (Chief Executive details kept permanently for historical purposes)	Limitations Act 1980	Head of HR

Expenses & overtime records	6 years after employment ceases	Taxes Management Act	Finance Director
Applications forms and interview notes (for unsuccessful candidates)	6 months following the closing date	Disability Discrimination Act 1995 and Race Relations Act 1976.	Head of HR
Statutory Maternity Pay records, calculations, certificates or other medical evidence	3 years after the end of the tax year in which maternity period ends	The Statutory Maternity Pay Regulations	Head of HR
Statutory Sick Pay records, calculations, certificates, self-certificates	3 years after the end of each tax year for Statutory Sick Pay purposes	Statutory Sick Pay (General) Regulations	Finance Director
Records relating to working time	2 years from date on which they were made	The Working Time Regulations	Head of HR
National minimum wage records	3 years after the end of the pay reference period following the one that the records cover	National Minimum Wage Act	Finance Director
DBS certificate information	6 months following appointment of the employee or volunteer	DBS code of practice, Section 122 of the Police Act 1997	Head of HR
Insurance			
Insurance Policies	3 years after lapse	Data Protection Act	HR Director
Claim Correspondence	3 years after settlement	Data Protection Act	HR Director
Employer's Liability insurance certificate	40 years	Employers' Liability (Compulsory Insurance) Regulations 1998	HR Director
Accident books, records/reports and health and safety records	3 years from the date of the last entry	RIDDOR	HR Director
Health & Safety Audits	3 years	RIDDOR	HR Director

Records documenting the investigation of accidents, dangerous occurrences and outbreaks of notifiable diseases on the institution's premises.	40 years	RIDDOR	HR Director
Volunteer and Support Group Activity Risk Assessments	3 years	Requirements of our Insurer	Head of Volunteer Development
Office Risk Assessments	3 years	Requirements of our Insurer	HR Director
Fundraising Event Risk Assessments	3 years	Requirements of our Insurer	Head of Fundraising
Patient Education and Health Professional Event Risk Assessments	3 years	Requirements of our Insurer	Head of Service Delivery
Supporter, Events and Promotional Information			
Contact and personal information related to members and beneficiaries	Permanently, marked inactive following 6 months of inactivity	Data retained to provide evidence of relationship with the beneficiary in case future legacy made.	Head of Fundraising
Biographies of Special Event attendees	12 months	Internal use - 1:1 meetings and events	Donor Relations Manager
Records of Health Professionals completing CPD accredited events or training	5 years following completion	Royal College of Practitioners Guidelines	Head of Professional Development
Master copy of publications	Permanently	For reference and historic records	Clinical Director
Recorded Calls	6 months	Training, quality and monitoring purposes	Human Resources Director
Contact and personal information related to volunteers	6 years following the end of their volunteer role	Limitations Act 1980	Head of Volunteer Development
Support Group Committee Meeting Minutes	Permanently	For 7 years to evidence financial decisions and thereafter for historical purposes.	Head of Volunteer Development
Compliance/Reporting information			

Certificates of destruction of confidential waste	3 years	To evidence secure destruction of confidential waste.	HR Director
Register of Complaints/Safeguarding/Serious Incident Reports/Data Protection Breaches, including relevant correspondence	10 years*	National Archives guidance	Head of Corporate Governance
Board of Trustees/Executive Directors/Committee Meeting Minutes	Permanently	Companies Act/Charities Act/Data Protection Act	Head of Corporate Governance
Internal meeting minutes, not including HR meetings	3 years*	Organisational benefit	Chairs of meetings
Approved Policies	3 years after being superseded	Limitations Act 1980	Head of Corporate Governance
Research Grant Applications			
Ongoing grants: Applications, CVs etc, Correspondence, Interim reports, Final reports, Financial documents, Email history, summary record of what applied for, when, and funding agreed.	For duration of grant, then see completed grants below	Needed for ongoing management of grants	Strategic Development Manager Research & Planning
Completed grants: Applications, CVs etc, correspondence, interim reports and email history	2 years from the end of the grant*	In case of queries or complaints	Strategic Development Manager Research & Planning
Financial documents	7 years from the end of the grant	For audit purposes and HMRC requirements	Strategic Development Manager Research & Planning
Summary record of what applied for, when, and funding agreed, and if not, the reasons why, and Final Reports of successful grants	Permanently*	For ongoing review of research strategy	Strategic Development Manager Research & Planning
Unsuccessful applications: applications, CVs, correspondence	6 months from closing date	In case of complaint	Strategic Development Manager

			Research & Planning
Research Grants Committee minutes	10 years from meeting date*	Decisions taken at meetings may relate to current grants	Strategic Development Manager Research & Planning
Research Grants Committee members, applications, CVs etc and correspondence	6 years from termination of office	In line with Volunteer records	Strategic Development Manager Research & Planning
Research Grants Committee members – failed applications	6 months from closing date	In case of complaint	Strategic Development Manager Research & Planning
Funding Applications			
Grant applications	To be reviewed after 20 years*	Organisational benefit	Trust Funding Manager
Monitoring reports	To be reviewed after 20 years*	Organisational benefit	Trust Funding Manager
The following are some guidelines for general correspondence and should be applied with common sense. Please speak to your Manager if you wish to make an exception to the below, outlining your reasoning.			
General correspondence			
Routine correspondence that requires no follow up or is considered to be a general enquiry	1 year*	Organisational benefit	All
Documentation related to internal processes	1 year after superseded*	Organisational benefit	All

Please note that there may be occasions when the above data is retained by the Charity for longer periods, for example when it is saved as part of a backup or as a deactivated file on the Charity database. On these occasions, access will be restricted and back-up files will be securely deleted when the system automatically overwrites data.

Appendix C: How data will be destroyed securely

Type of data storage	How data is stored securely	How it will be destroyed	Controls in place to ensure secure disposal	Who is responsible	Who is accountable
Electronic files on the G:Drive	Permissions are set to restrict access	Deletion from the server.	Regular review of the folders on the G:Drive.	Facilities & I.T. Manager	Executive Director – Corporate Services
Emails	Information Security Policy/Cyber Essentials	Deletion from the cloud.	Data Retention Policy on Outlook.	Facilities & I.T. Manager	Executive Director – Corporate Services
Personal and organisational data held on CRM	See Information Security Policy/CRM Policy/Cyber Essentials documentation	Deletion from the cloud.	Automatic rules on the system and manual deletion as required.	Database Manager, Head of Digital	Executive Director – Strategic Development
Computer hardware and external data storage e.g. USB drives, and includes recorded calls	Devices are password protected and USB drives are encrypted.	Third party supplier contracted to destroy hardware securely.	Certificate of destruction	Facilities & I.T. Manager	Executive Director – Corporate Services
Paper	Lockable cabinets are used to store all personal information. Only authorised personnel are permitted to access the premises with a door code system in place. Third party supplier provides off site storage of archived files.	Third party supplier contracted to empty confidential waste consoles regularly.	Contract with supplier, annual review of contract and certificates of destruction provided for each disposal. Time set aside by each team to review files, at a minimum of once per year.	Facilities & I.T. Manager	Executive Director – Corporate Services

Appendix D: Subject Access Request – What happens next?

Following receipt of a Subject Access Request the following steps will be taken:

1) Verify your identification

Often, we will have no reason to doubt a person's identity, for example, if we have regularly corresponded with them. However, we can ask Data Subjects to provide any evidence we reasonably need to confirm their identity. For example, we may ask them for a piece of information held in their records that we would expect them to know: a witnessed copy of their signature or proof of their address.

If the person requesting the information is a relative/representative of the data subject, then the relative or representative is entitled to personal data about themselves but must supply the individual's consent for the release of their personal data. If they have been appointed to act for someone under the Mental Capacity Act 2005, they must confirm your capacity to act their behalf and explain how they are entitled to access their information.

2) Collate the information

We will check that we have enough information in the request to find the records requested. If we feel we need more information, then we will promptly ask for this. We will gather any electronically held information (including emails) or hard copy information held in a Filing System. We will also identify any information provided by a third party or which identifies a third party.

If we have identified information that relates to third parties, we will write to them asking whether there is any reason why this information should not be disclosed. We do not have to supply the information unless the other party has provided their consent or it is reasonable to do so without their consent. If the third-party objects to the information being disclosed we may seek legal advice on what action we should take.

Before sharing any information that relates to third parties, we will where possible anonymise information that identifies third parties not already known to the individual, and redact information that might affect another party's privacy. We may also summarise information rather than provide a copy of the whole document.

3) Issuing our response

We will respond to the request within one month, following the resolution of any queries around the information requested. In certain circumstances, we may request up to two further months to provide the information, for example where the requests are complex. Copies of the information in a permanent form will be sent to the Data Subject except where they agree, where it is impossible, or where it would involve undue effort. In these cases, an alternative would be to allow the Data Subject to view the information on screen at the Charity.

We will explain any complex terms or abbreviations contained within the information when it is shared. Unless specified otherwise, we will also provide a copy of any information that the Data Subject has seen before.

Appendix E: Subject Access Request Form

Completion of this form assists us in fulfilling and processing your request.
Data Protection: These details are to be used only for the purposes of processing the Subject Access Request, contacting you with the information you have requested and verifying your identification. We will keep a record of this request for 10 years and then this information will be securely destroyed. For more details see the Policy Section on our website, www.theros.org.uk.

Name:	
Email:	
Phone:	
Address and post code:	
Nature of the request: If you wish to obtain information from a specific timeframe please make this clear where possible.	
Date:	

Please tick the following boxes, where relevant, to indicate for what reasons you have previously contacted the Royal Osteoporosis Society.

- ☐ Helpline
- ☐ Member of the Charity
- ☐ Made a donation
- ☐ Attended an event
- ☐ Requested a publication

☐ Previous employee, volunteer or trustee

Your request will be responded to within one month of submission.
Response to be sent via:

☐ Email

☐ Post (Signed for) to the address above unless otherwise indicated below

Delivery address:

……

……

……

Post Code: …….

Checking you are who you say you are

We will request some form of identity verification as part of the Subject Access Request process. This is to ensure that your information is only disclosed to authorised individuals.
For example, following submission of this form we will ask you to confirm one or more of the following, depending on your frequency of interaction with the Charity:

- Current address
- Date of Birth (members only)
- Membership Number (members only)
- Recent communication you received from the Charity
- A copy of your driving licence or passport.

If you wish to discuss your request further or see a full copy of our Subject Access Request Policy please contact us *dataprotection@theros.org.uk*