Data protection policy

This policy sets out what we do to protect individuals' personal data.

1. Purpose of the policy

1. Moorfields Eye Charity is committed to complying with privacy and data protection laws, as outlined in the EU-wide General Data Protection Regulation (retained in domestic law as the UK GDPR). This policy sets out what we do to protect individuals' personal information.
2. Anyone who handles personal data in any way on behalf of Moorfields Eye Charity, including employees, consultants, volunteers, partners and suppliers must ensure that they comply with this policy. Section 3 of this policy describes what comes within the definition of "personal data". Any breach of this policy will be taken seriously and may result in disciplinary action or more serious sanctions.
3. This policy may be amended to reflect any further changes in legislation, regulatory guidance or internal policy decisions.

2. About this policy

The Director of Finance and Resources is responsible for ensuring compliance with the UK GDPR and with this policy as the charity's data protection lead. Any questions or concerns about this policy should be referred in the first instance to the Director of Finance and Resources via the charity mailbox moorfields.eyecharity@nhs.net, or by calling the charity phone line on 020 7566 2565.

3. Definitions of data protection terms

The following terms will be used in this policy and are defined below:

1. Data subjects include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

2. Personal data means information relating to a living person who can be identified from that information (or from that information when combined with other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).
3. Data controllers are the people who, or organisations which, decide the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to process personal data in compliance with the UK GDPR. Moorfields Eye Charity is the data controller of all personal data as defined in the UK GDPR. Moorfields Eye Charity is the data controller of all personal data that we manage in connection with our work and activities.
4. Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include other organisations such as website or server hosts, fulfilment houses or other service provides which handle personal data on our behalf.
5. EEA is the European Economic Area which includes all countries in the European Union as well as Norway, Iceland and Liechtenstein.
6. ICO means the Information Commissioner's Office (the authority which oversees data protection regulation in the UK).
7. Processing is any activity that involves use of personal data. It includes obtaining, recording, holding, organising, amending, using, disclosing or destroying personal data.
8. Sensitive personal data (also known as Special Category data) includes information about a person's:

    - 8.1 racial or ethnic origin;
    - 8.2 political opinions;
    - 8.3 religious or philosophical beliefs;
    - 8.4 trade union membership;
    - 8.5 genetic and biometric data;
    - 8.6 physical or mental health or condition;
    - 8.7 sexual life or orientation; or
    - 8.8 criminal record (including any allegation that they have committed an offence).

4. Data protection principles

Anyone processing personal data must comply with the data protection principles as outlined in the UK GDPR. We are required to comply with these principles (detailed in sections 5-12 below) in respect of any personal data that we deal with as a data controller.

Personal data should be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
2. 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
4. 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 ('accuracy');
5. 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
6. 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 ('integrity and confidentiality');
7. not transferred to people or organisations outside the EEA without adequate safeguards being put in place.

5. Processing data fairly and lawfully

1. The first data protection principle requires that personal data is obtained fairly and lawfully, and processed for purposes that the data subject has been told about transparently.
2. To do this, every time we receive personal data about a person that we intend to keep, we provide that person with access to our Data Protection and Fair Processing policies. In other words, we are required to tell at the time that they provide use with their data:

    - 2.1 who will be holding their information, i.e. Moorfields Eye Charity – including contact details for how they can get in contact with us about their data;
    - 2.2 why the charity is collecting their information and what the charity intends to do with it (for example, to process donations or send mailing updates about our activities);
    - 2.3 the legal basis for collecting the personal data (for example, if the charity is relying on their consent, or on legitimate interests or on another legal basis);
    - 2.4 if the charity is relying on legitimate interests as a basis for processing what those legitimate interests are;
    - 2.5 whether the provision of their personal data is part of a statutory or contractual obligation and details of the consequences of the Data Subject not providing that data;
    - 2.6 the period for which their personal data will be stored or, where that is not possible, the criteria that will be used to decide that period;
    - 2.7 the existence of the rights of individuals (please see section 9 below for the rights that must be referred to);
    - 2.8 details of people or organisations with whom the charity will be sharing their personal data;
    - 2.9 where relevant, the fact that the charity will be transferring their personal data outside the EEA and details of relevant safeguards;
    - 2.10 the right to lodge a complaint with the Information Commissioner's Office;

- 2.11 the right to withdraw consent if consent is the lawful ground that has been relied upon; and
- 2.12 the existence of any automated decision-making including profiling in relation to that personal data.

3. Where the charity obtains personal data about a Data Subject from a source other than the Data Subject, the charity must provide information (in addition to the information set out at Section 5.2) on:

- 3.1 the categories of personal data; and
- 3.2 information on the source of the personal data and whether this is a publicly available source.

This information must be provided within a reasonable time period and no later than 30 days from when the data was first obtained, or upon first communication with the data subject if sooner.

4. This fair processing information is provided to our supporters in a number of places including on the Moorfields Eye Charity website, in mailings, promotional materials and application forms.

5. Obtaining an individual's consent can help to ensure we process their data fairly, but in most cases it is not required. In such circumstances, data will be processed (and collected) under the legal basis of legitimate interest. Moorfields Eye Charity may process an individual data subject's information under both the legal basis of consent or of legitimate interest, based on the form and purpose of processing.

6. These legal bases, as defined in the UK GDPR, are described as follows: [consent] the data subject has given consent to the processing of his or her personal data for one or more specific purposes; [legitimate interest] processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

6. Processing data for the original process

1. The second data protection principle requires that personal data is only processed for the specific purposes that the individual was told about when we first obtained their information. This includes forms of processing undertaken by Moorfields Eye Charity as are explained in our Fair Processing notice and policy.
2. This means that we should not collect personal data for one purpose and then use it for another, unless the second purpose is implicit. If new forms of processing are introduced by Moorfields Eye Charity, these will either be conducted under consent or legitimate interest. In the case of the latter, supporters will be directed to changes within the Fair Processing notice, allowing them to make an informed decision as to whether or not they wish to opt-out of that (or any) particular form of processing.

7. Personal data should be accurate

The third and fourth data protection principles require that personal data that we keep should be accurate, adequate and relevant. Inaccurate or out-of-date data should be archived if necessary or otherwise destroyed securely.

8. Not retaining data longer than necessary

1. The fifth data protection principle requires that we should not keep personal data for longer than we need it for the purpose(s) for which it is being processed. This means that the personal data that we hold should be destroyed or erased from our systems when it is no longer needed. If you think that we are holding out-of-date or inaccurate personal data, please speak to the Director of Finance and Resources, through the channels listed in section 2.
2. For guidance on how long particular types of personal data that we collect should be kept before being destroyed or erased, please contact the Director of Finance and Resources or seek legal advice.
3. It is the policy of Moorfields Eye Charity to regard personal data stored about the charity’s supporters and prospective supporters as necessary to support

ongoing fundraising process and legacy management activities of the charity. Therefore, Moorfields Eye Charity operate a policy not to routinely permanently delete personal data relating to its supporters or prospective supporters. This does not include information held for the purposes of gift administration (card numbers, expiry dates etc), which will not be held for longer than is necessary for the performance of contract, or as mandated by law.

4. Data Subjects (supporters, potential supporters, grant applicants etc) have the right to request that Moorfields Eye Charity delete any/all data held relating to them. In such instances where this is requested but it is also necessary for Moorfields Eye Charity to retain certain information (such as spending restrictions on a donation), information will be sufficiently anonymised (moved to an aggregate record for example) that the data subject cannot be identified from remaining information.

9. Rights of individuals under the UK General Data Protection Regulation (UK GDPR)

The UK General Data Protection Regulation (UK GDPR) gives people rights in relation to how organisations process their personal information. They include (but are not limited to):

1. Right of access. A data subject has the right:
    a. to obtain confirmation of whether the charity is processing their personal data;
    b. to request a copy of any personal data that the charity holds about them (as Data Controller);
    c. to be provided with: a description of the categories of information that he charity is processing; the purposes for which the information is used; details of anyone to whom their personal data has been disclosed; how long the data will be stored; to be told of the existence of the right to request rectification or erasure of personal data or restriction of processing or to object to such processing; the right to lodge a complaint with the Information Commissioner's Office; to be told, where any information is not collected from the person directly, any available information as to the source of the information; and, to be told of the existence of automated decision-making and meaningful

information about the logic involved in automated decision making as well as the significance and envisaged consequences of such processing to the individual.

2. Right to rectification. A data subject has the right to have inaccurate data amended.

3. Right to erasure (also known as the right to be forgotten). A data subject has the right to request that all of their personal data is erased (the right to be forgotten) in certain circumstances. However, even when those circumstances apply, there are exceptions which can allow a controller to refuse a right to erasure.

4. Right to restriction. A data subject has the right to restrict the processing of personal data.

5. Right to data portability. A data subject has the right to receive information relating to the processing of personal data in a commonly used format.

6. Right to object. A data subject has the right to object to the processing of data where the processing is based on either the conditions of public interest or legitimate interests.

7. Right not to be subject to automated decision-making based solely on automated processing which significantly affects the individual.

8. Requests from data subjects to exercise these rights may be received by email, telephone or written post. Data Subjects are instructed by the charity's Privacy Policy to direct their requests to the Director of Finance and Resources, but should any such request come straight to you, please contact the Director of Finance and Resources immediately.

9. Some of the rights only apply in limited circumstances and exemptions may be available. If you have any questions about whether or how the charity needs to exercise/facilitate a data subject's right, please speak to the Director of Finance and Resources.

10. Subject Access Requests (SARs)

1. Data subjects may make requests to access the personal data Moorfields Eye Charity holds about them. It is not mandatory for such requests to include the words ‘Subject Access Request’ and each case should be assessed individually.
2. If you are in any doubt as to whether you have received a Subject Access Request (SAR), or what information you should provide please contact the Director of Finance and Resources.
3. If the Director of Finance and Resources is satisfied that the charity must comply with a SAR, the requested information must be provided to the data subject without delay and at the latest, within at least one month of receipt of the request. However, where it is not possible from the content of the SAR to identify the relevant Data Subject or there is not enough information to identify the personal data in question, the charity is entitled to respond asking for further information.
4. Should a SAR come straight to you, please contact the Director of Finance and Resources immediately.

11. Data security

1. The sixth data protection principle under UK GDPR requires that we keep secure any personal data that we hold.
2. We are required to put in place procedures to keep the personal data that we hold secure.
3. When we are dealing with sensitive personal data (as defined in paragraph 3.8 above), more rigorous security measures are employed, for instance, if sensitive personal data is held on a memory stick or other portable device it must be encrypted.
4. When deciding what level of security is needed, our starting point should be to look at whether the information is sensitive or confidential and how much damage could be caused if it fell into the wrong hands.
5. The following security procedures must be followed in relation to all personal data processed by us:
    - Entry controls: Any stranger seen in entry-controlled areas should be reported.

- Equipment: Users should ensure that individual monitors do not show confidential information to others who are unauthorised and that they log off from or lock their PC when it is left unattended.
- Secure lockable desks and cupboards: Desks and cupboards should be kept locked if they hold confidential information of any kind. Personal information is always considered confidential.
- Confidential information should not be left on display on desks or work areas within the office.
- Methods of disposal: Paper documents should be shredded. Memory sticks, CD-ROMs and other media on which personal data is stored should be physically destroyed when they are no longer required.
- Backing up data: Daily back-ups should be taken of all data on our system; data should not be stored on local drives or removable media as these will not be backed up.
- Travelling with personal data and remote working: Staff must keep data secure when travelling or using it outside of our offices.

For instance, documents and laptops must be kept secure, (not left lying around off site); where you are using media that contains suitable software, you should make every effort to arrange for encryption (speak to Head of IT at Moorfields Eye Hospital); data stored on computers when working at home must be password protected, and kept confidential; when you are working from home, you should ensure that the laptop or computer you are using is securely protected from theft while you are away from it; and, secure exchange of data: personal data must always be transferred in a secure manner.

The degree of security required will depend on the nature of the data, the more sensitive and confidential the data, the more stringent the security measures should be. The following precautions should be taken:

- Use registered post or courier. Never send a CD or stick containing personal data by ordinary post.
- Use password protection (on files) if sending by email – but recognise this is not very secure and should only be used for small quantities of information.
- Never send sensitive data by email unless it has been encrypted (speak to Head of IT at Moorfields Eye Hospital for more details).

- If you wish to process personal data on your personal device (such as a smartphone or tablet) you need to be satisfied that it is being processed securely. Please discuss this with the Head of IT at Moorfields Eye Hospital before doing so.

12. Transferring data outside the EEA

1. The eighth data protection principle of the prior legislation (DPA) requires that when organisations transfer personal data outside the EEA they take steps to ensure that the data is properly protected. Similar provisions are contained within Articles 44-50 the UK GDPR. This is a principle with which Moorfields Eye Charity continues to comply.
2. The European Commission has determined that certain countries provide an adequate data protection regime. These countries currently include Andorra, Argentina, Canada, Guernsey, Isle of Man, Israel, New Zealand, Switzerland, Faroe Islands, Jersey and Uruguay, and this list may be updated.
3. As such, personal data may be transferred to people or organisations in these countries without the need to take additional steps beyond those you would take when sharing personal data with any other organisation. In transferring personal data to other countries outside the EEA (which are not on this approved list), it may be necessary to seek the consent of the individuals whose data is being transferred or to enter into an EC-approved agreement. If the recipient is based in the US, it will also be possible to transfer data if it is accredited under the EU/US Privacy Shield.
4. For more information, please speak to the Director of Finance and Resources or seek further legal advice.

13. Processing sensitive personal data

1. On some occasions we may collect information about individuals that is defined by the UK GDPR as sensitive, and special rules will apply to the processing of it. The categories of sensitive personal data are set out in the definition in section 3.
2. Purely financial information is not technically defined as sensitive personal data in active legislation; however, particular care should be taken when

processing such data, as the ICO is likely to treat a breach relating to financial data very seriously.

3. In most cases, in order to process sensitive personal data, we must obtain explicit consent from the individuals involved. As with any other type of information we will also have to be absolutely clear with people about how we are going to use their information.

4. It is not always necessary to obtain explicit consent. There are a limited number of other circumstances in which the Data Protection Bill permits organisations to process sensitive personal data (such as due diligence). If you are concerned that you are processing sensitive personal data and are not able to obtain explicit consent for the processing, please speak to the Director of Finance and Resources.

14. Notification

1. Our data protection policy/Fair Processing notice defines our data subjects (i.e. the people about whom we hold personal data), our data categories (the information we hold about them) and our purposes (the reasons why we hold this information). A copy of our notification may be viewed on request, through the Moorfields Eye Charity website, or online via the public register on the web site of the ICO (www.ico.org.uk).

2. We should only engage in processing which comes within the categories set out in this notification. Processing for additional purposes should not take place, except for within the circumstances outlined in section 6.2. This notification is reviewed once a year to ensure it is still accurate and up to date. If you think our notification needs to be updated to include additional processing, please contact the Director of Finance and Resources.

15. Consent

Whilst consent is not required to process most data, it is usually required to process sensitive personal data (see paragraph 12 above) and is required to send direct marketing by email or SMS, and where a telephone number is registered with the Telephone Preference Service – as outlined in the Privacy and Electronic

Communications Regulations (PECR) law. You should not undertake this activity without talking first with the Director of Finance and Resources.

16. Data breach/loss of personal data

In the event of a data breach or loss of personal data, Moorfields Eye Charity will report to the ICO, Charity Commission, and affected data subjects as appropriate. This will be done by the charity's Chief Executive. Such incidents will be reported to the ICO within a period of 72 hours – as outlined in the UK GDPR.

If a data subject feels that Moorfields Eye Charity has acted in a manner counter to the framework outlined throughout this policy, resulting in the loss of their personal data, they can lodge a formal complaint with the ICO directly.

Monitoring and review of the policy

This policy is reviewed annually by our Board of Trustees to ensure that it is achieving its objectives.

Last reviewed: June 2025