Data Protection / GDPR Policy

Adopted by Trustees: 13th May 2020

Reviewed: 22nd November 2024

Next Review: November 2026

Data protection is everyone's responsibility. To help protect people's personal data keep to these Dos and Don'ts:

- Always treat people's personal information with integrity and confidentiality
- Know what the data protection principles are and apply them
- Store hard copies securely and transfer them directly to recipients
- Use your organisation email address rather than send data to your personal email.
- Be alert to cyberattacks and report suspicious emails or calls
- Report losses of data or devices as soon as possible
- Before sending direct marketing, ask the Data Protection Officer (DPO) if this is appropriate
- Take care to use the 'bcc' option for bulk emailing
- Beware of autocomplete on email. Check you are sending to the right address
- Ensure your personal device has appropriate security measures if using it for work-related activity
- If you have a question about any data protection issue, ask the DPO

Policy

This policy sets out how Axminster and Lyme Cancer Support protects personal data that we process.

The security and management of data is important to ensure that we can function effectively and successfully for the benefit of our members and for the community and voluntary sector.

It is essential that people's privacy is protected through the lawful and appropriate use and handling of their personal information. The use of all personal data by Axminster and Lyme Cancer Support is governed by:

- The General Data Protection Regulation (GDPR)
- The UK Data Protection Act 2018 (DPA)

Every member of Axminster and Lyme Cancer Support has a responsibility to adhere to the Data Protection Principles outlined in the GDPR, and to this Data Protection Policy.

If you have a question about this Data Protection Policy or an area of concern about data protection matters, please contact our Data Protection Officer (DPO). **The DPO is Donna Drew.**

Data Protection Principles

There are six Data Protection Principles defined in Article 5 of the GDPR. These require that all personal data be:

- processed in a lawful, fair and transparent manner
- collected only for specific, explicit and limited purposes ('purpose limitation')
- adequate, relevant and not excessive ('data minimisation')
- accurate and kept up-to-date where necessary
- kept for no longer than necessary ('retention')
- handled with appropriate security and confidentiality.

We are committed to upholding the Data Protection Principles. All personal data under our control must be processed in accordance with these principles.

Lawful Processing

1. All processing of personal data must meet one of the six lawful bases defined in Article 6(2) of the GDPR:
   - Where we have the consent of the data subject
   - Where it is in our legitimate interests and this is not overridden by the rights and freedoms of the data subject
   - Where necessary to meet a legal obligation
   - Where necessary to fulfil a contract, or pre-contractual obligations
   - Where we are protecting someone's vital interests
   - Where we are fulfilling a public task, or acting under official authority

2. Any special category data (sensitive types of personal data as defined in Article 9(1) of the GDPR) must further be processed only in the line with one of the conditions specified in Article 9(2).

3. The most appropriate lawful basis will be noted in the Data Processing Register. (See below - Accountability).

4. Where processing is based on consent, the data subject has the option to easily withdraw their consent.

5. Where electronic direct marketing communications are being sent, the recipient should have the option to opt-out in each communication sent, and this choice should be recognised and adhered to by us.

Data Minimisation and Control

1. The data collection processes will be regularly reviewed by the Trustees to ensure that personal data collected and processed is kept to a minimum.

2. We will keep the personal data that we collect, use and share to the minimum amount required to be adequate for its purpose.

3. Where we do not have a legal obligation to retain some personal data, we will consider whether there is a business need to hold it.

4. We will retain personal data only for as long as it is necessary to meet its purpose.

5. In the case of sharing personal data with any third party, only the data that is necessary to fulfil the purpose of sharing will be disclosed.

6. Anonymisation of personal data stored or transferred should be considered where doing so is a possibility.

Accountability

1. Axminster and Lyme Cancer Support will maintain a Data Processing Register as required by Article 30 of the GDPR to document regular processing activities.

2. The 'Data Protection Officer' (DPO) has the specific responsibility of overseeing data protection and ensuring that we comply with the data protection principles and relevant legislation. (see below - Role of the Data Protection Officer).

3. The DPO will ensure that the Data Processing Register is kept up to date and demonstrates how the data protection principles are adhered to by our activities. Individual members of staff have a duty to contribute to ensure that the measures outlined in the Register are accurately reflected in our practice.

4. The Trustees monitor our compliance with relevant policies and regulatory requirements in respect of data protection as part of our Data Management Strategy.

5. All employees, volunteers, consultants, partners or other parties who will be handling personal data on behalf of Axminster and Lyme Cancer Support will be appropriately trained and supervised where necessary.

6. The collection, storage, use and sharing of personal data will be regularly reviewed by the Data Protection Officer and the Trustees.

7. We will adhere to relevant codes of conduct where they have been identified and discussed as appropriate.

8. Where there is likely to be a high risk to individuals rights and freedoms due to a processing activity, we will first undertake a Data Protection Impact Assessment (DPIA) and consult with the Information Commissioner's Office (ICO) prior to processing if necessary.

Use of Processors

1. Axminster and Lyme Cancer Support must only appoint processors who can provide sufficient guarantees around compliance with the GDPR and that the rights of data subjects will be protected.

2. Where a processor can demonstrate that they adhere to approved codes of conduct or certification schemes, this should be taken into consideration for choice of supplier.

3. Where Axminster and Lyme Cancer Support uses a processor, a written contract with compulsory terms as set out in Article 28 of the GDPR must be in place (plus any additional requirements that we determine). Processors can only act on the instruction of Axminster and Lyme Cancer Support.

Organisational Measures

1. All devices owned by Axminster and Lyme Cancer Support will have hardware encryption set up by default where possible, including laptops, mobile devices and removable media.

2. All staff, contractors, temporary workers, consultants, partners or anyone else working on behalf of Axminster and Lyme Cancer Support and handling personal data are bound by the data protection legislation and this Policy.

3. Where any contractor, temporary worker, consultant, or anyone else working on behalf of Axminster and Lyme Cancer Support fails in their obligations under this Policy, they shall indemnify Axminster and Lyme Cancer Support against any cost, liabilities, damages, loss, claims or proceedings that may arise from that failure.

Role of The Data Protection Officer

1. The Data Protection Officer role is assigned to a member of staff on a voluntary basis i.e. we are not legally obliged to have a DPO. We have chosen to do so as part of demonstrating our accountability and ensuring our compliance with data protection requirements.

2. The DPO assists Axminster and Lyme Cancer Support to:

- monitor our internal compliance
- inform and advise on our data protection obligations

- provide advice regarding Data Protection Impact Assessments
- act as a contact point for data subjects and the ICO.

3. The DPO advises the Trustees on data protection matters.

4. The DPO is easily accessible as a point of contact for data protection issues and is identified as the point of contact in our privacy notice and other external material.

5. The DPO identifies, organises and delivers training for Axminster and Lyme Cancer Support personnel.

6. The DPO is required to have appropriate knowledge of data protection law and best practice and is provided with adequate resources to help them carry out their role.

7. The DPO is nominally responsible for carrying out responses to requests made by data subjects, reporting breaches and drawing up policies and procedures.

Procedures for employees and Volunteers

While this policy helps us to demonstrate how we seek to comply with data protection legislation and be accountable for our actions, all personnel must comply with these procedures for processing or transmitting personal data.

- Always treat people's personal information with integrity and confidentiality. Don't hand out personal details just because someone asks you to.
- Where personal data exists as hard copy, it should be stored in a locked box, drawer or cabinet, and not left where anyone could access it.
- The transfer of hard copies should be passed directly to the recipient.
- The loss or theft of any device should be reported as soon as possible to the DPO, Systems Administrator or Head of Information Management.
- Take care when connecting to public wi-fi connections, as these can expose your connection to interception. If you are not sure if a connection is secure, do not connect to it.
- If you are thinking of sending marketing to individuals, consult with the DPO first, as there are certain laws that apply to electronic direct marketing. This could include anything that promotes the aims or purpose of Axminster and Lyme Cancer Support, including promoting an event or seeking engagement.
- Take care to email the intended recipient (especially where email address autocomplete is turned on). Use the 'bcc' field for emailing several people where using 'to' or 'cc' is not needed.
- These procedures and policies also apply to the use of remote access to Axminster and Lyme Cancer Support cloud systems. If you are using your own device to access personal data ensure that your device has a firewall and is password protected.
- If you do have a question or are unsure about any of these procedures, contact the Data Protection Officer.

Rights of Data Subjects

1. Under data protection laws, data subjects have certain rights:

- Right to be informed. The right to be told how their personal data is used in clear and transparent language.
- Right of access. The right to know and have access to the personal data we hold about them.
- Right to data portability. The right to receive their data in a common and machine-readable electronic format.
- Right to be forgotten. The right to have their personal data erased.
- Right to rectification. The right to have their personal data corrected where it is inaccurate or incomplete.
- Right to object. The right to complain and to object to processing.
- Right to purpose limitation. The right to limit the extent of the processing of their personal data.
- Rights related to automated decision-making and profiling. The right not to be subject to decisions without human involvement.

2. We will uphold individuals' rights under data protection laws and allow them to exercise their rights over the personal data we hold about them. Privacy information will acknowledge these rights and explain how individuals can exercise them. Most rights are not absolute, and the individual will be able to exercise them depending on the circumstances, and exemptions may apply in some cases.

3. Any request in respect of these rights should be made in writing to admin@axminsterandlymecancersupport.co.uk.

4. There is no fee for facilitating a request, unless it is 'manifestly unfounded or excessive' in which case administrative costs can be recovered.

5. Requests that are 'manifestly unfounded or excessive' can be refused.

6. We will take reasonable measures to require individuals to prove their identity where it is not obvious that they are the data subject.

7. We will respond to the request within one month from the date of request or being able to identify the person, unless it is particularly complex (in which case we will respond in no longer than 90 days).

8. The DPO will ensure that required actions are taken and that the appropriate response is facilitated within the deadline.

9. The DPO will draw up procedures for responding to requests where necessary, for example, for facilitating Subject Access Requests.

Reporting of Breaches

1. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

2. All personnel should be vigilant and able to identify a suspected personal data breach. A breach could include:

- loss or theft of devices or data, including information stored on USB drives or on paper

- hacking or other forms of unauthorised access to a device, email account, or the network
- disclosing personal data to the wrong person, through wrongly addressed emails, or bulk emails that inappropriately reveal all recipients email addresses
- alteration or destruction of personal data without permission

3. Where a member of staff discovers or suspects a personal data breach, this should be reported to the DPO as soon as possible.

4. Where there is a likely risk to individuals' rights and freedoms, the DPO will report the personal data breach to the ICO within 72 hours of the organisation being aware of the breach.

5. Where there is also a likely high risk to individuals' rights and freedoms, Axminster and Lyme Cancer Support will inform those individuals without undue delay.

6. The DPO will keep a record of all personal data breaches reported and follow up with appropriate measures and improvements to reduce the risk of reoccurrence.