Data Protection Policy

Introduction and Scope

This policy outlines Axminster Hospital League of Friends commitment to data protection and compliance with the UK Data Protection Act. The purpose of this policy is to ensure that all personal data held by the charity is processed lawfully, fairly, and transparently, and that the rights of data subjects are protected. This policy applies to all individuals working on behalf of Axminster Hospital League of Friends, including Trustees, employees, and volunteers.

Data Protection Lead

Axminster Hospital League of Friends will appoint a Data Protection Lead who will be responsible for overseeing data protection and leading on any incident investigation and reporting. The Data Protection Lead will also ensure that all staff and volunteers are provided with any induction, on the job or other training and made aware of their data protection responsibilities.

Data Protection

Data protection is the practice of safeguarding personal information by applying data protection principles and complying with the Data Protection Act. The Data Protection Act is a UK law that regulates the processing of personal data. The UK Information Commissioner's Office (ICO) provides guidelines on data protection that [Charity Name] will follow.

UK GDPR: The UK General Data Protection Regulation, which outlines the rules for processing personal data in the UK.
Data Processor: An individual or organisation that processes personal data on behalf of a data controller.
Data Controller: An individual or organisation that determines how and why personal data is processed.
Data Subject: An individual whose personal data is being processed.
Processing: Any operation performed on personal data, including collection, storage, use, and disclosure.

Personal Data: Any information that can identify a living individual, such as name, address, or email address.
Sensitive Personal Data: Personal data that requires extra protection, such as health information or ethnic origin.
Direct Marketing: Any communication aimed at promoting a product or service directly to an individual.
PECR: The Privacy and Electronic Communications Regulations, which govern electronic direct marketing.
Valid Consent: Consent given freely, specifically, and informed, and can be withdrawn at any time.
Legitimate Business Purpose: A lawful reason for processing personal data that is necessary for the legitimate interests of the data controller or a third party.

Data protection principles

Data is:

- Processed lawfully, fairly and in a transparent manner.
    - There are several grounds on which data may be collected, including consent.
    - We are clear that our collection of data is legitimate and we have obtained consent to hold an individual's data, where appropriate.
    - We are open and honest about how and why we collect data and individuals have a right to access their data.
- Collected for specified, explicit and legitimate purposes and not used for any other purpose.
    - We are clear on what data we will collect and the purpose for which it will be used.
    - And only collect data that we need.
    - When data is collected for a specific purpose, it may not be used for any other purpose, without the consent of the person whose data it is.
- Adequate, relevant and limited to what is necessary.
    - We collect all the data we need to get the job done.
    - And none that we don't need.
- Accurate and, where necessary, kept up to date.
    - We ensure that what we collect is accurate and have processes and/or checks to ensure that data which needs to be kept up-to-date is, such as beneficiary, staff or volunteer records.
    - We correct any mistakes promptly.

- Kept for no longer than is necessary. We understand what data we need to retain, for how long and why.
    - We only hold data only for as long as we need to.
    - That includes both hard copy and electronic data.
    - Some data must be kept for specific periods of time (eg accounting, H&SW).
    - We ensure that data no longer needed is destroyed.
- Processed to ensure appropriate security, not only to protect against unlawful use, but also loss or damage.
    - Data is held securely, so that it can only be accessed by those who need to do so. For example, paper documents are locked away, access to online folders in shared drives is restricted to those who need it, IT systems are password protected, and/or sensitive documents that may be shared (eg payroll) are password protected.
    - Data is kept safe. Our IT systems have adequate anti-virus and firewall protection that's up-to-date. Staff understand what they must and must not do to safeguard against cyber-attack, and that passwords must be strong and not written down or shared.
    - Data is recoverable. We have adequate data back-up and disaster recovery processes.

Individual Rights

We recognise that individuals' rights include the right to be informed, of access, to rectification, erasure, restrict processing, data portability and to object.

Use of Imagery/Video

All imagery is protected by copyright and cannot be used without the consent of the owner, usually the person who took the image.

We will let people know that images are being recorded by including the details in event sign-up or ticketing information, by making an announcement at the start of the event, or by including the advice in a programme. If the event is more informal, or outside, then clear notices explaining that photographs/videos will be taken will be displayed.

Today's event is being photographed and filmed. Axminster Hospital League of Friends will be using these images to create an internal record of the project. The images may be used in future publicity, on our website or on our social media. If you don't want to be included, please talk to the Manager.

If a person can be identified from a photo or video, then it is classed as personal data we will treat it like any other personal data. Individuals and groups will be asked for their consent to share their image on publicity, social media and/or website. All images will be deleted after five years.

When using images consideration should be given to the following:

- Is the image sensitive personal data? If it is, do you have the individual's consent?
- For small groups and individuals, has an image consent form been used?
- People under 13 years of age are not legally able to give consent. When using images of children, has appropriate consent been granted?
- Some people are unable, or may be unable to give consent, and this must be obtained from the person who is able to make decisions on their behalf, such as a Lasting Power of Attorney. Any decisions that you may make on their behalf, must always be in their best interests.
- When using images of children or other vulnerable people, are you confident your use of the image will not place them at risk? Particularly, if it is to be used publicly, such as in the Media or on the web.
- When photographing large groups, have the individuals been given a chance to opt out of the photograph?
- Has the person/people in the image been told how the image will be used?
- Are you using the image according to how the person/people were told it would be used?

Fundraising

We will ensure that our fundraising complies with the Data Protection Act and ICO guidelines and also the Fundraising Regulator guidelines including, if applicable, direct marketing and PECR. We will respect the privacy and contact preferences of our donors. We will respond promptly to requests to cease contacts or complaints and act to address their causes.

Data Breach

A breach is more than only losing personal data. It is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

We will investigate the circumstances of any loss or breach, to identify if any action needs to be taken. Action might include changes in procedures, where there will help to prevent a re-occurrence or disciplinary or other action, in the event of negligence.

We will notify the ICO within 72 hours, of a breach if it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals. For example:

- Result in discrimination.
- Damage to reputation.
- Financial loss.
- Loss of confidentiality or any other significant economic or social disadvantage.

Approval and Review

Version No	Approved By	Approval Date	Main Changes	Review Period
1.0	Trustees	Feb 2024	Initial draft approved	Annually