Little Hearts Matter
Half a heart, not half a life

Little Hearts Matter Data Policy

Little Hearts Matter takes the responsibility for the collection, use, storage and protection of data very seriously.

Data Protection is actually the protection of people and the charity's ethos is the support of individuals at their most vulnerable. There are many instances when the protection of personal data overlaps with confidentiality. The charity will work to protect personal information and information on personal situations with equal vigour.

Personal information held by Little Hearts Matter as a hard copy or within an electronic or relevant manual filing systems must be kept safe and specific permission to use the data to contact individuals, provide services or use the data for research must be gained from each individual. Some permission is gained as part of membership of the organisation; other permission is sought as a specific agreement. For example the use of data for marketing or the use of data, photographs and/or stories for support, awareness or publicity.

The following policy has been written in line with the needs of the charity's members, children, supporters, volunteers, professional associates, trustees and staff and the charity's values and in parallel with statutory data regulations. This policy will be formally reviewed and updated yearly or in line with statutory change.

Caring, thoughtful, mindful, open and honest, empowering, creative, nurturing, resourceful

The Little Hearts Matters data promise

- **To Prevent Harm - All personalised data will be collected, stored and accessed with care and appropriateness.**
- **Accuracy - Only accurate data will be collected and stored. The charity will have a responsibility to ensure that data is updated as appropriate and that only data needed to offer LHM services and/or to remain in contact with members is retained.**
- **Transparency – the members will have access to the Data Policy and can ask to see any of the data held about them or their child (until they reach the age of 18).**
- **Choice – all Stakeholders will be offered choice about how their data is used and can request to change the status of their data and its use at any time.**
- **Little Hearts Matter will not pass on or sell any membership data to a third party. If services are required from a third party permission will be sought to pass information on from the person being referred.**
- **The only occasions when information about an individual may be passed on without their permission is when they are deemed to be at risk of harm either from themselves or another or if they are a risk to another or when there is a legal obligation to do so.**

A copy of this Data Policy will be kept within the Governance and Staff Handbook sections of the main server.

A further copy will be made available for members in the governance section of the open Little Hearts Matter website.

LHM Data

Little Hearts Matter holds a number of different types of data both electronically and as hard copies. The organisation works to create links between different member, child and young adult information and, where relevant, fundraising and marketing data. The aim is to minimise repeating information.

Membership information: parent, carer or grandparent information that allows us to contact them about support and information services from the time of membership application. This includes name, address, email, telephone number and consent for how they wish to be contacted by the charity. This data is linked to the data held about their child to enable age and diagnosis related information to be available. Individual agreement will be sought to allow personal stories or photos to be used to aid awareness or offer member to member support.

Adults with Single Ventricle Heart Disease Members: LHM holds information that allows us to contact them about support and information services from the time of membership application or from the time they move from childhood membership to adult membership. This includes name, address, email, telephone number and consent for how they wish to be contacted. Information on their heart condition, treatments and treatment unit. information on Disability Allowance claims, PIP, school or education reports, medical reports, employment records and consent on how they would like to be contacted by the charity. (Individual agreement will be sought to allow personal stories or photo's to be used to aid awareness or offer member to member support.)

Child or young adult Member:- Children and young adults under the age of 18 with a single ventricle heart condition. LHM holds information that allows us to offer and inform them of support or information services. Name, address, telephone number, email (theirs or their parents), information on their heart condition, treatments and treatment unit. Information on a Disability Living Allowance claims, school reports, medical reports. Individual agreement will be sought from parents to allow personal stories or photo's to be used to aid awareness or offer member to member support. Children over 13 but under 18 will need to give their permission for data to be used in parallel with their parents.

When a child member turns 18 they will be offered the opportunity to become full members. A letter of invitation and an action to seek contact permission will be sent out to each individual.

Associate Members :- Anyone affected by a diagnosis of a single ventricle heart condition or involved in the treatment or day to day life of a young member.

- Extended family members
- Medical professionals
- Educational professionals
- Parents or adults with SVHD living abroad.

Information held – name, home or professional address, email address, information about the child their membership relates to or the hospital, school or work place that relates to their link with SVHD. We also retain information on how they would like to be contacted.

Research Volunteers: Members, associate members, child members and other interested individuals may choose to take part in research that relates to:

- The role of the charity
- Their medical health, treatment or history

- The psychological impact of their condition
- Lifestyle issues related to their condition

Personal data relating to them as individuals will be required as part of the study. Information that relates to how they wish to be contacted and their permission relating to how the results of the study will be communicated will be stored with their personal data.

Volunteers: Little Hearts Matter has a number of different types of volunteer. Support, advocacy, fundraising and general administration. The charity holds information to enable us to contact and thank them as well as to ensure they can take part in on-going training. Many of the volunteers are members. The data retained is name, address, email and telephone number. We retain information on how they would like to be contacted.

Donors/Fundraisers: any individual or a named person from an organisation that has fundraised for or donated to the charity. The information held may be all or some of the following: name, address, email telephone number, bank details, links to members or child members, name of organisation and details of the permission and style of contact they want from the charity. This is used to thank, formally report and keep the individual or organisation up to date on the work of the charity and how donations are used.

Professional Contacts: A number of health, educational, governmental, 3rd sector and business individuals work with the charity. The personal information held about them relates to how they have asked to be contacted: name, address, email, telephone number.

Trustees: Individual's contact information is collected and stored to enable the charity to provide the Governance according to the charity's Aims and Objectives, produce transparent accounts and to report to the Charity Commission and Companies House. The Information stored is name, address, date of birth, email, telephone number, conflicts of interest.

Staff: Individual data relating to the staff to support their employment, records of past employment and bank details, next of kin and conflicts of interest are stored as part of their employment.

Data Law

There are a number of legal, statutory rules that set down the data compliance needed by UK charities.

There are six Principles six of General Date Protection Regulation, GDPR. This is a European Directive (this will still stand when the UK leaves the EU)

The Statutory Body policing the uses and protection of data is the Information Commissioning Organisation headed by the Information Commissioner. https://ico.org.uk/

There is also an expectation from the Government and the Charity Commission that charities will be highly responsible and professional in the way that data is sued to collect information, funds or opinions.

GDPR Principles

(a) processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) 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 not be considered to be incompatible with the initial purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) 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;

(e) 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 in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

(f) 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.

Article 5(2) requires that

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Confidentiality

The ethical principle of confidentiality requires that information shared by a member, child or young adult, with the charity's support team in the course of offering support, information or guidance is not shared with anyone that does not sit within the Service Team (a combination of Service focused Trustees and staff) This principle promotes an environment of trust.

There are important exceptions to LHM's confidentiality promise, namely where it conflicts with a duty to warn or duty to protect. This includes instances of suicidal behavior or homicidal plans, child abuse or dependent adult abuse. See the Little Hearts Matter Safeguarding Policy.

Little Hearts Matter works to train all members of the support and administration team on the collection and use of members personal information, who to contact when there are concerns and how to report in a safe and confidential way.

As some of LHM's support work is remote it is important to ensure good communication between team members but vigilant protection of personal data and information. *See Data Protection below*. All information that relates to member contact must be sent by email to designated LHM email address. The information will be stored, whilst it is needed to offer service, then destroyed once it is no longer relevant.

LHM Membership Data Collection Policy

Clearly it is important that the charity has access to personal details that allow the organisation to offer support and relevant information relating to the membership, and their related children. Focussed specialised support can only be provided by knowing details of medical, educational and social service provision. The collection of this information forms part of membership. Terms and Conditions of Membership are available at the time of application. Consent is also sought on how best the charity can contact individual members and what information the organisation has permission to send out.

Members, Associate Members and Children's details are submitted:

- Online via the website application process
- Via hard copy application form received in the post
- Via the phone when support is being sought. (Consent can be given verbally but must be recorded as such.)

The day to day inputting of membership related data is the responsibility of the Data Processor. Any member of staff can add data or information to the database if they are offering support or information to the member. When adding data it is important to ensure that care is taken to make sure the data is accurate, only pertains to the issue relating to support or information services and is not phrased in a derogatory way.

Details relating to individual's consent to contact with the charity and requests for support and or information will be stored in personalised sections of the database.

The database is password protected within a restricted section of the database. It cannot be accessed remotely. The database is backed up daily to an external Cloud repository which is password protected and encrypted. A secondary back up is taken as an encrypted hard copy which is locked within a fire and waterproof safe within the LHM office.

Any data collected for the purpose of future contact or research will be consented for on an individual basis.

- Social Media – LHM has a full consent policy relating to the use of pictures and personal stories that are used on the main Social Media sites.
- Photo or story permission – LHM has a consent process by which permission is given to use photographs and personal stories as awareness tools.
- Child Protection. – LHM has a full Safeguarding Policy in place.
- Research Consent – LHM is involved in collecting the voice of its members as well as encouraging involvement in external research projects. The use of personalised information will always be explained as part of the research consent process.

Members will be offered an opportunity to update their information formally on a two year basis, during the bi-annual member consultation. Informally members will be asked to update their information via the newsletter, email and social media.

Trustee, Staff, Interns and Volunteer Data

Part of employment, even voluntary, is handing over personal information that ensures you are remunerated and that you can be kept safe whilst at work. There is a need for references pertaining to previous employment and information relating to appraisal and performance during employment.

As a children's charity there is a need to ensure that DBS checks are performed on staff and volunteers so data pertaining to permission and personal information is needed to qualify the Safeguarding Policy.

Staff and volunteers have an on call role, protecting their personal contact details by providing dedicated telephones and safe limits on personal contact information is essential. This forms part of the Staff Handbook.

Hard copies of personal information pertaining to staff, payroll and appraisal is stored within a locked cabinet only accessible by the Chief Executive. All documented information on personnel issues stored electronically is only saved to the CE's password protected laptop and backed up to a closed file on the Server.

Payroll and employment documentation is stored by the Finance team on designated and password protected computers. Hard copies are stored in locked cabinets.

Documentation is stored for 6 months after a member of staff has left in case of comment or complaint. The data will then be archived for a further 3 years in accordance with HMRC recommendations. It may be needed for reference or financial audit.

Job Applications

Information from unsuccessful job applicants will be kept for 6 months to offer an opportunity for feedback. They will then be destroyed.

Data consent – the right to opt out.

Membership, Associate Membership, Child and Young Adult Membership of the charity refer to the Terms and Conditions of the organisation. These Terms and Conditions allow for the collection of personal and sensitive data. They allow the restricted use of personal data when the organisation is working to offer support and information services.

The use of that data for Marketing Purposes or Research or Awareness of the charity's work requires an added, specific, consent which is requested at the time of membership application or as part of a specific project.

Members consent is on three levels:

- Consent to membership – access to support and information services.
- Consent to membership but restricted consent to mail outs, this relates to bereavement.
- Consent to membership and to being contacted about all charity activity and marketing.

Associate Membership consent on two levels:

- Consent to associate membership – access to support and information
- Consent to associate membership and to being contacted about all activity and marketing.

The status of each individual member's consent then creates the direction and type of any further contact. No member will be denied support when requested whatever their consent level.

Routes to contact:

- Post
- Email
- Telephone

The right to access to personal data by the Data Subject

Personal Data is not the sole property of the organisation that holds it. The individual that it pertains to has every right to ask to see anything stored about them, they are the Data Subject.

If a request to see data, full or partial, is received from the Data Subject the Data Controller (see named person below) must provide a permanent intelligible copy of all personal data, hard copy and electronic copy retained about them.

The data controller can withhold third party material, especially if a duty of confidentiality is owed, this means that if data is revealed that includes information about another person it could break their confidentiality

Although the data controller can charge up to £10 to provide data, Little Hearts Matter would wave charges for a request from a member, associate member, child or young adult member.

Following the formal request from a Data Subject the information they have requested must be with them within 40 days.

Marketing/Fundraising data

All communication and marketing materials sent to fundraisers should be distributed to those individuals who have acknowledged and indicated to the charity that they are happy to receive such materials (i.e. have "opted in").

As a lot of the information regarding individuals who fundraise for Little Hearts Matter is received through Just Giving, the information given here (e-mail addresses, phone numbers etc.) should be the only data used by the charity unless further details are given separately or specific permission is given by the individual concerned. Just Giving has its own Privacy Policy that as a charity registered to them, LHM must adhere to - www.justgiving.com/info/privacy and www.justgiving.com/info/charities-terms-and-conditions

If the charity has received an individual's contact details through JustGiving, Virgin Giving and related fundraising portals then – even if we have their details by other means - these are the only details Little Hearts Matter will use. Sharing of JustGiving pages for promotion of the amount raised or request for funding will only be done by mutual agreement between the fundraiser and Little Hearts Matter.

If a photo or story was to be used for a specific fundraising or marketing campaign that would involve higher than usual exposure (social media posts, flyers, posters etc.) then specific permission will be sought from the member and/or family involved.

Direct requests for funding should not form part of marketing materials to individuals who have not "opted in". These include e-mail footers, website banners and direct e-mail, including e-newsletters. However, indirect requests taking visitors to a different webpage with a direct request for funding is satisfactory.

The charity receives a number of financial details from fundraisers including bank details, especially when setting up standing order payments. Any bank details received that need to be kept by LHM are kept in a secure file, both electronically and on a paper copy; the details are never shared with anyone and destroyed as soon as they're no longer needed or the standing order is cancelled. –Direct donations are paid into CAF Online who pledge to "not share information about a Donor with any outside person or organisation, except where this has been authorised by the Donor or a person acting with their authority or where this is required in order to provide a product or service to the Donor, or where CAF is legally obliged to do so".

Payments for fundraising and promotional materials are received through PayPal. PayPal's Privacy Policy can be found on its website: https://www.paypal.com/ie/webapps/mpp/ua/privacy-full

Financial Data

The charity holds a great deal of information about member, and friends of the charity, banking and financial details, relating to their donations, fundraising and Gift Aid. The protocol for the collection, storage, protection and use of this data is set out in the Fundraising section of this policy.

The organisation also has Staff and Trustee banking details relating to the Payroll and the paying of expenses. These are stored within password protected computers. Information about personal banking details are only sent between LHM designated email addresses. Hard copies of the data are stored in locked filing cabinets

It is essential to respect this type of data.

Information relating to standing orders, invoices, and purchase details are stored within locked cabinets. Most of the information is not personal but the organisation follows the same policy of keeping all financial information safely locked away to ensure that there are no breaches of data loss.

Facebook and Social Media Data

All closed Social Media sites require users to submit their personal contact details as a method of membership confirmation. These are stored within the social media site and accessed by the charity's service and administration team.

Some personal details are sometimes used on the open Social Media sites. Full permission to use the information must be granted, especially the use of photos or personal stories.

Personal permission statement

Any photos or stories we receive will go in to the LHM archive and may be used in any of our publications in the future. They will also be posted on Facebook. By sending us your photos and stories you agree for us to use them in this way. If you would prefer us not to use them on social media, on the LHM Blog or within LHM publications please let us know as soon as possible. It is important that you are aware, photos and stories used on the internet are public and can be viewed by anyone, anywhere in the world. We will not post your surname with the photo but may post your child's first name, age and heart condition if we have this information.

The name of the person giving permission and the name of the child is then stored within a file in LHM shared documents.

Permission to use film or picture footage from events is sought at each event. The documents are retained by the Information Administrator for use when any publications are produced.

Data Storage, Security and Confidentiality

Data Storage

Personal Information is stored by the charity in many ways.

- Hard copy data

Membership details and confidential information must be stored in locked filing cabinets and the keys are stored in a Key Safe that only the charity staff have access to. This includes membership application forms, details about a child or sibling, their medical, social care and education information.

Any hard copy membership, child or young adult responses to research projects or feedback relating to LHM events will be locked in filing cabinets and the key stored in the Key Safe.

Staff and Volunteer information will be stored in a locked filing cabinet that only the CE and the Administration Manager have access to. Keys to this cabinet will be kept in a separate bespoke key cabinet.

All hard copies of member, child or young person, friend of the charity, staff, Volunteer or Trustee financial information is locked away. The keys to this information are stored in a locked key cabinet. Only the charity's staff, Treasurer or Vice Treasurer have access to this information.

Any notes made during a conversation about support or information must be up loaded on to the members electronic or hard copy data and stored as above. Notes must be shredded.

- Electronic

Electronic membership, child or young adult data is stored, as part of the charity's database, on the main server of the Little Hearts Matter IT system. The database is password protected. All members of staff are able to access the main database when they are logged on to their individually password protected personal computer, whilst working in the office.

Any notes made during a conversation about support or information must be uploaded on to the individual member's electronic or hard copy data and stored as above. Notes must be shredded immediately once data has been uploaded.

Sections of the main database, finance data or correspondence relating to members or donators may be used for projects, reporting or service work and may be downloaded on to individual team members computers. These computers are password protected.

All individual computers have security systems set within their day to day function. Software Anti Virus, Firewall protection updates occur automatically when the computers are connected to the server.

Individual passwords are updated every six months.

All staff computer content is backed up to the main server every time a team member works in the main office. The encrypted backup drives are alternated and are stored in a fire and flood protected safe in the office. The key to the safe is locked away in the key cupboard.

Staff computers will shut down after 15 mins of no use and require password re-entry. All staff must formally shut down their computers at the end of the day. Any portable devices must be locked away and keys to the computer storage locked in the Key Safe.

If staff work remotely computers must be transported safely. All laptops must be password protected.

Staff must not hold any LHM data on personal, non-Little Hearts Matter device.

Little Hearts Matter will look to provide dedicated laptops and phones for all staff who work away from the office.

The charity's main database and financial database are backed up to a Microsoft remote Cloud. Backup to this Cloud occurs at 11pm each night and notification of successful back up is emailed to the staff team's joint email address. A record of the backup is made daily on working days. Password protected access to the Cloud stored information is only held by the administration team and the Treasurer and Vice Treasurer.

A second, encrypted USB copy of the database is stored in the fire and waterproof safe.

Little Hearts Matter have the support of an external IT company, BDR. If BDR need access to any of the staff's computers they have to ask for permission. They have signed a confidentiality agreement with regards to any LHM data.

The storage of photographs of children or young people can only occur if permission from a parent or guardian has been obtained. Copies of their permission and the photos are stored on the main LHM shared mainframe but may also be stored on individual, password protected, team member's computers.

Electronic staff data is retained by the Chief Executive on their personal computer. It is password protected and backed up to the main server when the CE is working in the main office.

<u>Remote working</u>

Data safety and member confidentiality requires that work done on laptops, remotely, must not include anything where a member can be identified by anyone who does not work for the charity.

Telephone calls to members must be done in a private space.

Conversations about members or child and young adult members must only be undertaken in a safe environment.

Information about a member or their circumstances can only be given to a third party with their permission and only if it can support their personal advocacy or improve their treatment of access to support.
If their experience is being used to validate a concern or to improve a service it must be used anonymously. If there is a concern that a member, child or young adult may be recognised during a conversation that conversation must stop.

Any notes made during a conversation about support or information must be uploaded on to the individual member's electronic or hard copy data and stored as above. Notes must be shredded.

Staff and Volunteer Training and Trustee awareness and responsibility

It is essential that all members of staff and volunteers have a full understanding of the data and confidentiality rules set out by Little Hearts Matter.

Data Policy training will form part of the bi-annual staff training policy. This will require individual staff members to sign to say that they have received training and understand the policy.

The use of scenarios and involvement in data reviews and discussions about confidentiality will form part of all members of staff training.

Induction: Instruction on the Data Policy will form part of all new staff member's training.

All Trustees will be involved in the annual review of the Data Policy and one named Trustee will take Board responsibility for adherence to the Policy.

<u>Staff Ethic</u>

Any member of the staff or volunteer team will need to adhere to the safe collection, use and storage of data but they will also have to be professional in the way they use the data the organisation collects.

- They need to respect the needs of the charity's members, associate members, children and young adults and respect the aims and ethos of the charity.
- They should not talk about individual members, their experiences, concerns or fears to anyone outside the organisation
- They must not share details of passwords to documents or computers that they should not have access to.

- They should not search through data that is not needed for their specific job.
- They should not allow anyone to access documents, seek out data or alter data that does not have approval to do so.

It is a Criminal Offence to:

- **Knowingly or recklessly access data you are not authorised to access.**
- **Knowingly or recklessly allow another person unauthorised access.**

Removal of Data

Little Hearts Matter is committed to the removal of data once it is no longer required or once permission to retain it is no longer consented.

Members who request to be removed from the database will no longer have contact from the charity. Their data will be stored as inactive for two years, and then removed. The reason for a two year period of retention is because many parents initially ask to be inactive after the death of a child or a change in personal circumstances. This is often reverted after a period of no contact.

On turning 18 a child member must become an adult member or decline to become a member. They will be contacted to ask for permission to retain their personal data and for permission to contact them. If the charity is unable to contact the individual their data will be stored as inactive for two years and then destroyed. If they remove permission their data will be stored for 6 months and then removed.

Financial information, accounts, donations, payments or invoices will be stored for 7 years.

Staff data will be retained in the office for six months for use in comment or complaint and then archived for 3 years in accordance with HMRC rules, for financial reference.

The charity will work to update data when information is given to the organisation by members or fundraisers.

Information about health professionals, associate professional members or third sector support teams will be reviewed yearly and information updated accordingly.

<u>Disposal of Data or Confidential Information</u>

Formal annual review of archived data, review of stored data, and review of membership status data will lead to the need to formally dispose of data.

Hard copy data will be shredded internally and the shredding's disposed of in the office rubbish.

Electronic Data must be deleted.

A record of the process of review and disposal will be kept within the Governance documentation.

Email

There are two areas of email use that require added policy information:

The use of LHM email addresses.

The charity will only use dedicated Little Hearts Matter emails to pass on details of financial, payroll or personal member details or service needs within the organisation. No information will be passed to non-LHM email addresses.

All members of the LHM team, staff, Trustees and volunteers will have a dedicated email address.

Marketing

As emails are addressed to specific recipients the use of Fundraising or Marketing banners will be restricted to people where permission has been received for this style of contact.

Little Hearts Matter's Data Controller

The overall responsibility for the data policy sits with the Little Hearts Matter Board of Trustees, day to day management of data issues would be taken by the staff and Finance and General Purposes team.

The named Trustee with Data responsibility is Peter Turner. In his absence the responsibility would be taken by Peter Groves.

The Data Controller

Suzie Hutchinson – Chief Executive

Responsibilities:

- Briefing the board on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other staff on tricky Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Notification
- Handling subject access requests
- Approving unusual or controversial disclosures of personal data
- Approving contracts with Data Processors

Supported by:

Tina Walmsley – Administration Manager

The Data Processors

Paula Hughes – Membership Data Processor

Peter Groves and David Baumber – Payroll Data Processor

Reporting a Data Breach

Under the Data Protection Act (DPA), there is no legal obligation on data controllers to report breaches of security, however the recommendation from the Information Coordinator is that serious breaches should be reported to the ICO.

Little Hearts Matter's position would be that if any of the following occur the Data Controller would contact the ICO.

A serious breach would include:

- Ransomware attack of the computer.
- Viral attack of any computers.
- The stealing of the data backup drives or encrypted files.
- The stealing of an LHM computer.
- Unauthorised access to the main LHM computers.

- Staff misuse of data that affects the status of the charity.

Penalties

The Regulation mandates considerably tougher penalties than the DPA: organisations found in breach of the Regulation can expect administrative fines of up to 4% of annual global turnover or €20 million – whichever is greater. Fines of this scale could very easily lead to business insolvency. Data breaches are commonplace and increase in scale and severity every day.