DATA PROTECTION POLICY

POLICY MONITORING	
Person responsible for Policy	Data Protection Officer: Chief Executive
Committee responsible for Review	Board of Trustees
Policy approved	February 2023
Frequency of Review	Annually
Date of next Review	February 2024

Policy statement

Lymphoma Action is responsible for appropriately managing personal data. The purpose of this policy is to ensure personal information received or obtained by Lymphoma Action is managed and used responsibly, securely and fairly and in accordance with data protection legislation.

Lymphoma Action collects and processes data in accordance with the General Data Protection Regulation 2016 (GDPR). This came into force to protect people's "rights and freedoms" and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

Lymphoma Action will ensure staff and volunteers are trained and aware of their responsibilities, as appropriate, in accordance with the requirements of GDPR and the Data Protection Act. The GDPR and this policy apply to all personal data processing functions, including those performed on beneficiaries, volunteers, staff, suppliers and partners personal data, and any other personal data the organisation processes from any source.

Regulatory framework and legislation

Lymphoma Action will comply with the following (and any other appropriate) legislation:

- The Data Protection (Processing of Sensitive Personal Data) Order 2000
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- The Human Rights Act (1998)
- The Regulation of Investigatory Powers Act (2000)
- The Freedom of Information Act (2000)
- The Health and Social Care Act (2015)
- The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) (2016)
- The Data Protection Act (2018)

Roles and responsibilities under GDPR

The Trustees and the Senior Management team (SMT) are responsible for the implementation and maintenance of this policy to ensure compliance with the GDPR.

Lymphoma Action is a Data Controller under the GDPR. As a data controller Lymphoma Action determines the purposes and means of processing personal data and has a legal obligation to demonstrate compliance with GDPR.

Data processors (staff and volunteers) are responsible for processing personal data on behalf of the controller. GDPR places specific legal obligations on the processor to maintain records of personal data and processing activities. In the case where the data processor is external to Lymphoma Action i.e. a third party, the defined data processor will have legal liability if responsible for any data breach.

The Data Protection Officer (DPO): this is a role specified in the GDPR, and is the Chief Executive Officer. The DPO is accountable to the Trustees for the management of personal data and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

I. Development and implementation of the GDPR as required by this policy,
II. Development and implementation of information security measures as per the Information Security policy.

The DPO has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and is the first point of call for staff and volunteers seeking clarification on any aspect of data protection compliance.

The DPO is also responsible for reviewing any associated registers and process documents regularly and may delegate some aspects of operational management e.g. training, to other members of the team as appropriate.

Staff and volunteers: Compliance with data protection legislation is the responsibility of all staff (whether permanent, temporary or contracted) and volunteers of the charity. Staff and volunteers are responsible for ensuring that they are aware of and comply with the requirements of this policy and the policies, procedures and guidance produced to support it.

Staff will receive training in data protection and use of personal data on appointment and regularly thereafter. Volunteers will receive regular communications. The day-to-day responsibilities for providing guidance to staff, volunteers and contractors will be undertaken by the relevant line managers.

Staff and volunteers are responsible for ensuring that any personal data about them and supplied by them to the charity is accurate and up-to-date.

Third parties: No third party may access personal data held by Lymphoma Action without having signed a contract of service that covers data protection, or entered into a specific data confidentiality agreement, which imposes on the third-party obligations no less onerous than those to which the charity is committed.

Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR.

1. Personal data must be processed lawfully, fairly and transparently

Lawful – identify a lawful basis before you can process personal data. Lymphoma Actions' lawful bases for processing data fall into one or more of the following and are documented in our privacy notices:

- *Consent:* has been given to Lymphoma Action to process their personal data for a specific purpose
- *Contract:* the processing is necessary for Lymphoma Action to do what the individual has requested
- *Legal obligation:* the processing is necessary for Lymphoma Action to comply with the law
- *Vital interests:* the processing of the data is necessary to protect someone's life
- *Public task:* the processing is necessary to perform a task for our official functions
- *Legitimate interests:* the processing is necessary for Lymphoma Action's legitimate interests.

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.

Transparently – the GDPR rules place an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

The specific information that must be provided to the data subject must, for example as part of the Lymphoma Action privacy statement, include:

- the identity and the contact details of the controller or their representative;
- the contact details of the Data Protection Officer;
- the purposes and legal bases of the intended processing of personal data
- the period for which the personal data will be stored;
- the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions relating to exercising these rights;
- the categories of personal data concerned;
- the recipients or categories of recipients of the personal data, where applicable;
- where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
- any further information necessary to guarantee fair processing.

2. Personal data can only be collected for specific, explicit and legitimate purposes

Data obtained for specified purposes must not be used for a purpose that differs from that for which it was collected. The Record of Processing Activity records the purpose and basis of processing for all processes.

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.

3. Personal data must be adequate, relevant and limited to what is necessary for processing

Lymphoma Action will not collect information that is not strictly necessary for the purpose for which it is obtained. All data collection forms (electronic or paper-based) must include a fair processing statement or link to privacy statement. The privacy notices are available to view on the Lymphoma Action website: https://lymphoma-action.org.uk/about-us-how-we-work-policies-and-terms-use/privacy-policy-and-cookies

All new processes will be assessed using the Data Processing Impact Assessment (DPIA), before implementation to ensure processing of personal data is appropriate, and limited to what is necessary and the outcomes will be summarised in the DPIAs spreadsheet.

For processing that is likely to result in a high risk to the rights and freedoms of data subjects, the DPIA must be signed off by the DPO before processing commences.

The DPO shall, if there are significant concerns, escalate the matter to the Trustees.

4. Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

i. Every reasonable step must be taken to ensure that personal data which is inaccurate, (having regard to the purposes for which it is processed), is erased or rectified without delay.

ii. The DPO is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

iii. It is also the responsibility of the data subject to ensure that data held by the charity is accurate and up to date. Forms will include validation to assist this, where appropriate.

iv. Staff and volunteers are required to notify the charity of any changes in circumstance to enable personal records to be updated accordingly.

v. The DPO is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate (taking into account relevant factors), and that retentions dates are reviewed and data which is no longer required is deleted.

vi. The DPO is responsible for responding to requests for rectification from data subjects within one month as per the Subject Access Request Procedure. This can be extended to a further two months for complex requests. If the charity decides not to comply with the request, the DPO must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

vii. In the unlikely case that personal data has been passed to a third-party and is subsequently found to be inaccurate or out of date, the DPO is responsible for informing the third-party and for passing any correction to the personal data to them where this is required.

5. Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

   i. Where personal data is retained beyond the retention date for a legitimate business reason, it will be pseudo-anonymised or summarised, as far as is practicable, in order to protect the identity of the data subject in the event of a data breach.

   ii. Personal data will be retained in line with the Retention of Records Procedure and, once its retention date is passed, it must be securely destroyed.

   iii. The DPO must specifically approve any data retention that exceeds the retention periods defined in Retention of Records Procedure and must ensure that the justification is clearly identified and logged.

6. Personal data must be processed in a manner that ensures the appropriate security

   i. All data processing activities will be assessed using a risk assessment to help minimise the risk to an acceptable level. Risks shall be viewed from the point of view of the data subject as well as that of the charity and the DPO will review overall risk profiles to identify any further measures needed.

   ii. To ensure technical security the charity has and will maintain Cyber Essentials certification, and will take any other security measures deemed necessary including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, as laid out in the Information and Communication Technology (ICT) Security Policy.

   iii. All Staff and Volunteers are responsible for ensuring that any personal data that they are responsible for is kept securely and is not, under any conditions, disclosed to any third party unless that third party has been specifically authorised to receive that information and has entered into a confidentiality agreement.

   iv. All personal data shall be held securely. Personal data shall be accessible only to those who have a legitimate requirement to use it. Who has access to what will be determined by the DPIA covering the relevant business process.

Data subjects' rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them, taken from the legislation:

   i. The right to be informed (our privacy statement details how data is collected and used)

   ii. The right of access. Individuals can apply to access their personal data (see Subject Access Requests)

iii. The right to rectification. Should the DPO receive notification from an individual that their personal data is inaccurate this will be rectified if possible or a supplementary statement added to their data

iv. The right to erasure. Lymphoma Action acknowledges the individuals' rights to be forgotten and requests received by the DPO will be considered and responded to within one calendar month

v. The right to restrict processing. Lymphoma Action will consider a request to the restriction or suppression of personal data processing. If the request is appropriate the DPO will supervise the appropriate changes to restrict the data

vi. The right to data portability. Information provided to Lymphoma Action will be available for the individual to move, copy or transfer easily from one IT environment to another in a safe and secure way, without affecting its usability

vii. The right to object. Our privacy statement details how individuals can object to the processing of their data under certain circumstances

The charity ensures that data subjects may exercise these rights:

They can make data access requests as described in Subject Access Request Procedure. This procedure also describes how we ensure that our response to the data access request complies with the requirements of the GDPR. Requests received either verbally or in writing will be recorded and responded to within one calendar month. Lymphoma Action recognises Subject Access Requests may be made to any member of the organisation and that no fee will be charged for reasonable requests: How to deal with a request for information: a step-by-step guide | ICO

They have the right to complain to us about the processing of their personal data. Such a complaint will be handled according to the Complaints Procedure.

Consent

Lymphoma Action has a clear policy for gaining consent via the appropriate forms depending upon the data processing reason. Consent has to be explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them. See the procedure.

viii. 'Explicit' means that there is a clear communication from the individual demonstrating active consent. This will be achieved by 'opt-in' choices on consent forms, which have to be ticked to give consent.

ix. 'Informed' means that the individual has sufficient information available to them to make the decision to consent. This will be achieved by clear wording on consent forms, and ensuring they have access to our privacy policy.

x. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

The data subject can withdraw their consent at any time.

Where the data subject is a child, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 13 (to be confirmed once legislation is enacted).

Where Lymphoma Action relies on legitimate interest in lieu of consent for certain postal communications, it will identify the legitimate interest, show why it is necessary and balance it against the individual's interests, rights and freedoms.

Data Breaches and incidents

Lymphoma Action will follow the data breach/incident notification procedure (appendix B) and will investigate all reported instances of actual or potential breaches of confidentiality and security. These will also be reported to the Information Commissioners Office where required: https://ico.org.uk/for-organisations/report-a-breach/

Under the Charity Commission's serious incident reporting guidance, data breaches or loss should also be reported to the Charity Commission and other regulatory bodies depending on the nature of the breach: https://www.gov.uk/guidance/how-to-report-a-serious-incident-in-your-charity

This policy applies to all those doing work for Lymphoma Action, including staff, volunteers, and suppliers. Any breach of the GDPR or this Policy may be dealt with under the disciplinary policy.

Disclosure of data

Personal data is only transferred or disclosed to third-parties where there is an appropriate Data protection agreement in place, usually as part of a contract or Non-Disclosure Agreement.

Personal data shall not be disclosed to unauthorised third parties. It is the responsibility of all staff to ensure this does not happen.

There are some instances when data has to be disclosed to a third party, such as the police. In these instances, the advice of the DPO must be sought before acting on any request.

Retention and disposal of data

The charity will not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

Data may be stored for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. It will be summarised or pseudo-anonymised to safeguard the rights and freedoms of the data subject.

The retention period for each category of personal data is set out in the Retention of Records Procedure along with the criteria used to determine this period including any statutory obligations for the retention of the data.

Personal data must be disposed of securely to prevent retrieval of the data later.

Data transfer outside the European Economic Area

Lymphoma Action is a UK only charity and does not transfer personal information, as defined by the GDPR, outside of the EEA.

In the exceptional circumstance that such a transfer is being contemplated, explicit, written, agreement must be obtained from the trustees, who must be assured that all requirements of the GDPR are met, particularly in the contract between the charity and the relevant 3rd party.

Document Owner and Approval

The DPO is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above. The DPO is also responsible for monitoring and putting in place such audit measures as necessary to ensure that this policy and associated procedures are followed.

Appendix 1 – Definitions used (mainly drawn from the GDPR)

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – The legal entity who determines the purposes and means of the processing of personal data, i.e. the charity. Referred to as 'controller' in this document.

Data processor – Any organisation processing data on behalf of a Data Controller.

Data protection officer – The individual responsible for the oversight of data protection in the charity, who reports to the chair of trustees on data protection matters, see section 3.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation(s) which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Data incident – this may be a security incident or an event that leads to a violation of the Charity's security policies and puts sensitive data at risk of exposure. All data **breaches** are security **incidents**, but not all security **incidents** are data **breaches**.

Personal data breach – an incident which is a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent – means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – The UK defines a child as anyone under the age of 13 years old. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

ICO – information commissioner's office – The organisation responsible for the enforcement of GDPR and where data breaches are reported.

January 2021. Re-approved February 2023

For new staff to sign:

By signing this document, you are accepting this agreement and agreeing to carry out your work or role in accordance with Lymphoma Action's Data Protection Policy and any other related policies and procedures.

Failure to comply with the Data Protection Policy will be treated as a disciplinary matter. In relation to all questions about data protection, the Chief Executive or a member of the senior management team should be consulted without delay.

Signed: **Date:**

Position: Date of appointment:

Please sign electronically and email to n.kinchin-smith@lymphoma-action.org.uk for retention on your HR file