

LUPUS UK Data Protection Procedures

1. Introduction

This document, along with LUPUS UK's Privacy Policy (available in full at www.lupusuk.org.uk/privacy-policy) sets out the obligations and procedures of LUPUS UK regarding data protection and the rights of data subjects in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "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.

These policies and procedures set LUPUS UK's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by LUPUS UK, its employees, volunteers, contractors, or other parties working on behalf of the charity.

2. Specified, Explicit, and Legitimate Purposes

2.1 LUPUS UK collects and processes personal data including;

2.1.1 Personal data collected directly from data subjects ; and

2.1.2 Personal data obtained from third parties.

2.2 LUPUS UK only collects, processes, and holds personal data for the specific purposes set out in its Privacy Policy (or for other purposes expressly permitted by the GDPR).

2.3 Data subjects are kept informed at all times of the purpose or purposes for which LUPUS UK uses their personal data.

3. Adequate, Relevant, and Limited Data Processing

LUPUS UK will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed).

4. Accuracy of Data and Keeping Data Up-to-Date

4.1 LUPUS UK shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject.

4.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

5. **Data Retention**

5.1 LUPUS UK shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

5.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it.

5.3 LUPUS UK will maintain records of donors, fundraisers, sponsors and lapsed members for a maximum of six years, as required for financial records and audit.

6. **Secure Processing**

LUPUS UK shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

7. **Data Security - Transferring Personal Data and Communications**

LUPUS UK shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

7.1 All digital documents containing personal data which are sent by email should be password protected. The password should be provided in a separate email.

7.2 Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using a Recorded Delivery postal service.

8. **Data Security - Storage**

LUPUS UK shall ensure that the following measures are taken with respect to the storage of personal data:

8.1 All electronic copies of personal data should be stored securely using passwords;

8.2 All physical removable media (such as USB Drives) that contain electronic copies of personal data should be password protected.

8.3 All hardcopies of personal data should be stored securely such as in a locked box, drawer, cabinet or office.

8.4 The LUPUS UK database containing all personal data stored electronically should be backed up daily with back-ups stored offsite. All backups should be password protected/encrypted.

8.5 Personal data may only be transferred to devices belonging to volunteers, contractors, or other parties working on behalf of LUPUS UK where the party in question has signed an agreement to comply fully with the letter and spirit of this Policy and of the GDPR.

9. **Data Security - Disposal**

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be deleted and disposed of. Paper copies should be properly shredded and any physical removable media (such as USB Drives or Hard Drives) which are disposed of should be damaged with a hammer to prevent potential retrieval of deleted data.

10. **Data Security - Use of Personal Data**

LUPUS UK shall ensure that the following measures are taken with respect to the use of personal data:

- 10.1 No personal data may be transferred to any volunteers, contractors, or other parties, whether such parties are working on behalf of LUPUS UK or not, without the authorisation of Paul Howard (CEO);
- 10.2 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, volunteers, sub-contractors, or other parties at any time;
- 10.3 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and
- 10.4 Where personal data held by LUPUS UK is used for marketing purposes, it shall be the responsibility of Paul Howard (CEO) to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service.

11. **Data Security - IT Security**

LUPUS UK shall ensure that the following measures are taken with respect to IT and information security:

- 11.1 User access control (with password protection) on files, folders and databases.
- 11.2 Remote access to National Office PCs will require two-step verification with a unique code generated for each log-in sent to the employee's mobile phone.
- 11.3 Anti-Virus, anti-spam, adware/spyware protection on each National Office PC/laptop and server.
- 11.4 Encrypted backups to external drives.
- 11.5 Regular security updates to server and National Office PCs.
- 11.6 Server to be monitored by Page Computer Services checking regularly for any problems and applying updates when critical ones are released.
- 11.7 All passwords are required to be changed every 90 days. Passwords must be constructed according to the following specifications:
 - Passwords must be a minimum of 10 characters
 - Passwords should include at least one symbol/non-standard character (for example, & £ @ etc.)
 - Passwords should not use dictionary words – you may substitute numbers for the letters (i.e. zero for O, 3 for E, etc.)
- 11.7 All software (including, but not limited to, applications and operating systems) shall be kept up to date. LUPUS UK shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so; and
- 11.8 No software may be installed on any LUPUS UK-owned computer or device without the prior approval of the Paul Howard (CEO)

12. **Data Breach Notification**

- 12.1 All personal data breaches must be reported immediately to LUPUS UK's Data Protection Officer.

- 12.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
- 12.3 In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.
- 12.4 Data breach notifications shall include the following information:
 - 12.4.1 The categories and approximate number of data subjects concerned;
 - 12.4.2 The categories and approximate number of personal data records concerned;
 - 12.4.3 The name and contact details of LUPUS UK's Data Protection Officer (or other contact point where more information can be obtained);
 - 12.4.4 The likely consequences of the breach;
 - 12.4.5 Details of the measures taken, or proposed to be taken, by the charity to address the breach including, where appropriate, measures to mitigate its possible adverse effects.
- 13. **Accountability and Record-Keeping**
 - 13.1 LUPUS UK's Data Protection Officer is Paul Howard (CEO), paul@lupusuk.org.uk, 01708 731251.
 - 13.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, LUPUS UK's other data protection-related policies, and with the GDPR and other applicable data protection legislation.
 - 13.3 LUPUS UK keep internal records of all personal data collection, holding, and processing, which incorporates the following information:
 - 13.3.1 The name and details of LUPUS UK, its Data Protection Officer, and any applicable third-party data processors;
 - 13.3.2 The purposes for which LUPUS UK collects, holds, and processes personal data;
 - 13.3.3 Details of the categories of personal data collected, held, and processed by LUPUS UK, and the categories of data subject to which that personal data relates;
 - 13.3.4 Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
 - 13.3.5 Details of how long personal data will be retained by LUPUS UK; and
 - 13.3.6 Detailed descriptions of all technical and organisational measures taken by LUPUS UK to ensure the security of personal data.
- 14. **Data Protection Impact Assessments**
 - 14.1 LUPUS UK shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the

rights and freedoms of data subjects under the GDPR.

14.2 Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

14.2.1 The type(s) of personal data that will be collected, held, and processed;

14.2.2 The purpose(s) for which personal data is to be used;

14.2.3 LUPUS UK's objectives;

14.2.4 How personal data is to be used;

14.2.5 The parties (internal and/or external) who are to be consulted;

14.2.6 The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

14.2.7 Risks posed to data subjects;

14.2.8 Risks posed both within and to LUPUS UK; and

14.2.9 Proposed measures to minimise and handle identified risks.

15. **Keeping Data Subjects Informed**

15.1 LUPUS UK shall provide the Privacy Policy to every data subject:

15.1.1 Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

15.1.2 Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose.

16. **Data Subject Access**

16.1 Data subjects may make requests at any time to find out more about the personal data LUPUS UK holds about them, what it is doing with that personal data, and why.

16.2 Employees wishing to make a request should do so to Paul Howard (CEO).

16.3 Responses to requests shall normally be made within one month of receipt, however this may be extended by up to two months if the request is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

16.4 LUPUS UK does not charge a fee for the handling of normal requests. LUPUS UK reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

17. **Rectification of Personal Data**

17.1 Data subjects have the right to require LUPUS UK to rectify any of their personal data that is inaccurate or incomplete.

17.2 LUPUS UK shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the charity of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

17.3 In the event that any affected personal data has been disclosed to third parties,

those parties shall be informed of any rectification that must be made to that personal data.

18. Erasure of Personal Data

18.1 Data subjects have the right to request that LUPUS UK erases the personal data it holds about them.

18.2 Unless LUPUS UK has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

18.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

19. Restriction of Personal Data Processing

19.1 Data subjects may request that LUPUS UK ceases processing the personal data it holds about them. If a data subject makes such a request, LUPUS UK shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

19.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

20. Objections to Personal Data Processing

20.1 Data subjects have the right to object to LUPUS UK processing their personal data based on legitimate interests, direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

20.2 Where a data subject objects to LUPUS UK processing their personal data based on its legitimate interests, the charity shall cease such processing immediately, unless it can be demonstrated that its legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

20.3 Where a data subject objects to LUPUS UK processing their personal data for direct marketing purposes, the charity shall cease such processing immediately.

20.4 Where a data subject objects to LUPUS UK processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the GDPR, "demonstrate grounds relating to his or her particular situation". LUPUS UK is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

21. Organisational Measures

LUPUS UK shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

21.1 All employees, volunteers, contractors, or other parties working on behalf of the charity shall be made fully aware of both their individual responsibilities and

LUPUS UK's responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;

- 21.2 Only employees, volunteers, sub-contractors, or other parties working on behalf of the charity that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by LUPUS UK;
- 21.3 All employees, volunteers, contractors, or other parties working on behalf of LUPUS UK handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
- 21.4 All personal data held by LUPUS UK shall be reviewed periodically.

22. **Transferring Personal Data to a Country Outside the EEA**

22.1 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

22.1.1 The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;

22.1.2 The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

22.1.3 The transfer is made with the informed consent of the relevant data subject(s);

22.1.4 The transfer is necessary for the performance of a contract between the data subject and LUPUS UK (or for pre-contractual steps taken at the request of the data subject);

22.1.5 The transfer is necessary for important public interest reasons;

22.1.6 The transfer is necessary for the conduct of legal claims;

22.1.7 The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

22.1.8 The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

23. **Implementation of Policy**

This Policy shall be deemed effective as of 21/05/2021. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: Paul Howard

Position: CEO

Date: 21/05/2021

Signature:

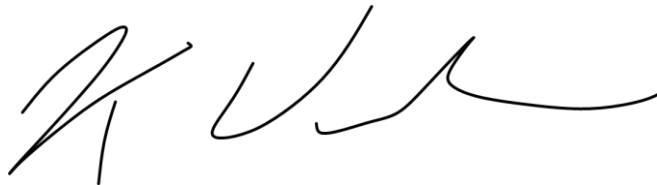
A handwritten signature in black ink, appearing to be 'PH', written on a light blue background.

Name: Kevin Weston

Position: Chair

Date: 17/06/2021

Signature:

A handwritten signature in black ink, appearing to be 'K Weston', written on a light blue background.

Due for Review by: Paul Howard

October 2022