Lay Community of St Benedict
Data Protection Policy

Charity Number 1100638

CONTENTS

Data Protection Policy

To be read in conjunction the following LCSB policies

Social Media Use
Safeguarding
Serious Situations and Sanctions

1 Overview

1.1 The Lay Community of St Benedict (LCSB) takes the security and privacy of personal information seriously. The LCSB recognises that its communications are now branching out across several social media platforms (particularly via Zoom). Users need to have regard for Data Protection regulation and ensure that great care is taken at all times, and all media, especially where personal information is disclosed. As part of our activities we need to gather and use personal information about a variety of people including members, former members, employees, office-holders and generally people who are in contact with us. The Data Protection Act 2018 (the "2018 Act") and "UK GDPR" regulate the way in which personal information about living individuals is collected, processed, stored or transferred. Any data protection breach must be brought to the attention of the Data Protection Officer immediately. (See para 10).

1.2 This policy explains the provisions that we will adhere to when any personal data belonging to or provided by data subjects, is collected, shared, processed, stored or transferred on behalf of the LCSB. We expect everyone processing personal data on behalf of the LCSB (see paragraph 5 for a definition of "processing") to comply with this policy in all respects.

1.3 The LCSB has a Data Protection Notice which is published on the LCSB website and within the LCSB Address Book. See annex 1.

1.4 It is intended that this policy is fully compliant with the 2018 Act and the UK GDPR. If any conflict arises between those laws and this policy, the LCSB intends to comply with the 2018 Act and the UK GDPR.

1.5 Any deliberate or negligent breach of this policy by an employee of the LCSB may result in disciplinary action being taken in accordance with our disciplinary procedure. It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see Paragraph 12 below) and such conduct by an employee would amount to gross misconduct which could result in dismissal. In the event of a Member making a deliberate or negligent breach of this policy, procedures may be brought through the LCSB's 'Serious Situations and Sanctions' policy.

1.6 In order to manage data protection compliance within the LCSB, the LCSB as a charity is recognised as the 'controller'. As a data controller, the LCSB has been registered in the register maintained by the Information Commissioner's Office (ICO) under the Data Protection Act 2018.

Controllers can delegate the processing of personal data to data processors, but the responsibility for keeping it safe will still rest with the controller. In order to manage date within the LCSB, the LCSB employs a Date Protection Officer and recognises selected Members as 'authorised processors'. The authorised processors are:

- Digital Evangelist
- Outreach Team Leaders
- Web communications Team Leader
- Leader of the LCSB
- Treasurer
- Finance and Bookings Secretary
- Authorised users of the LCSB CAF bank account
- Finance Team (when finance appeals are made from time to time)

"You're a processor if you're only acting on behalf of the instructions of a controller – if a business has hired you to process their mail, for example. As a processor, you wouldn't be doing anything with the data if the controller hadn't asked you to. It's not up to you to decide what should happen to it, which means you're only processing the information and not controlling it. However, you do have responsibilities to protect the personal data that you've been trusted with and to use it appropriately in-line with your contract with the controller." ICO

2 Data Protection Principles

2.1 Personal data will be processed in accordance with the seven '**Data Protection Principles**.' It must:

- be processed fairly, lawfully and transparently; using personal data in a way that complies with the law, and in a way that our members, staff and other users expect and have been told about.
- be collected and processed only for specified, explicit and legitimate purposes; only use personal data for the reasons we have collected it, and not for something extra or unrelated.
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed; limiting the amount of personal data we collect to what we need.
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- Storage limitation – personal data should not be kept for longer than is necessary for the purposes for which it is processed; when it is no longer needed, it should be securely destroyed or deleted.
- be processed securely. Personal data needs to be kept securely. We will make sure that the details of staff, members and those who use our services is protected.

- Accountability: taking responsibility, having appropriate measures in place and keeping records to demonstrate how we achieve data protection compliance.

We are accountable for these principles and must be able to demonstrate compliance.

3 Definition of personal data

3.1 **"Personal data"** means information which relates to a living person (a "data subject") who can be identified from that data on its own, or when taken together with other information which is likely to come into the possession of the data controller. It includes any expression of opinion about the person and an indication of the intentions of the data controller or others, in respect of that person. It does not include anonymised data.

3.2 This policy applies to all personal data whether it is stored electronically, on paper or on other material or social media platform.

4 Definition of special category personal data

4.1 '**Special category personal data**' is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; genetic or biometric data; data concerning physical or mental health; or data concerning a person's sex life and sexual orientation. Special category data is personal data that needs more protection because it is sensitive. In addition, the LCSB will hold financial records and information regarding LCSB personnel and would regard this as 'sensitive' and treated as such. Pastoral information held by the LCSB will also be treated as 'sensitive' by the LCSB.

4.2 A significant amount of personal data held by the LCSB will be classed as special category personal data, either specifically or by implication, as it could be indicative of a person's religious beliefs.

5 Definition of processing

5.1 **'Processing'** means any operation which is performed on personal data, such as collection, sharing, recording, organisation, structuring or storage; adaption or alteration; retrieval, consultation or use; disclosure by transmission, dissemination or otherwise making available; and restriction, destruction or erasure.

6 How personal data should be processed

6.1 Everyone who processes data on behalf of the LCSB has responsibility for ensuring that the data they collect and store is handled appropriately, in line with this policy.

6.2 Personal data should only be accessed by those who need it for the work they do for or on behalf of the LCSB. Data should be used only for the specified lawful purpose for which it was obtained. Data processors will be responsible for periodically ensuring that access to the data they hold will be held and shared only with other authorised persons. Data processors will also be responsible for bringing this policy to the attention of volunteers with whom they share data.

6.3 The legal bases for processing personal data (other than special category data, which is referred to in Paragraph 7 below) are that the processing is necessary for the purposes of the LCSB's legitimate interests; or that (so far as relating to any staff whom the LCSB employs) it is necessary to exercise the rights and obligations of the LCSB under employment law; or that (in relation to the processing of personal data relating to criminal convictions and offences or related security measures in a safeguarding context) the processing meets a condition in Part 1, 2 or 3 of Schedule 1 of the Data Protection Act 2018.

6.4 Personal data held in all ordered manual and electronic files and databases should be kept up to date. It should be shredded or disposed of securely when it is no longer needed. Unnecessary copies of personal data should not be made.

7 When is consent needed for the processing of personal data?

7.1 A significant amount of personal data held by the LCSB will be classed as special category personal data, as it could be indicative of someone's religious beliefs.

7.2 Processing of such special category data is prohibited under the UK GDPR unless one of the listed exemptions applies. Three of these exemptions are especially relevant (although others may also apply):

- the individual has given **explicit consent** to the processing of the personal data for one or more specified purposes; OR

- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside that body without the consent of the data subjects; OR

- processing is necessary for reasons of substantial public interest, and in particular for the purpose of (a) protecting an individual from neglect or physical, mental or emotional harm; or (b) protecting the physical, mental or emotional well-being of an individual, where that individual is either aged under 18 or is aged 18 or over and is "at risk" (has needs for care and support, experiencing or at risk of neglect or any type of harm, and unable to protect themselves).

7.3 Most of the processing carried out by the LCSB will fall within the latter two exemptions, and will be carried out by the LCSB with appropriate safeguards to keep information safe and secure. This information will not be disclosed outside the LCSB without consent. Such processing will not require the explicit consent of the data subject.

7.4 Where personal data is to be shared with a third party, the LCSB will only do so with the explicit consent of the data subject. For example, personal data will only be included in a directory for circulation or included on a website where consent has been obtained.

7.5 If consent is required to process the information this should be recorded. If consent is given orally rather than in writing, this fact should be recorded in writing.

8 Keeping personal data secure

8.1 Personal data should not be shared with those who are not authorised to receive it. Care should be taken when dealing with any request for personal information over the telephone, social media or otherwise. Identity checks should be carried out if giving out information to ensure that the person requesting the information is either the individual concerned or someone properly authorised to act on their behalf.

8.2 Hard copy personal information should be stored securely (in lockable storage, where appropriate) and not visible when not in use. Filing cabinets and drawers and/or office doors should be locked when not in use. Keys should not be left in the lock of the filing cabinets/lockable storage.

8.3 Passwords should be kept secure, should be strong, changed regularly and not written down or shared with others.

8.4 Emails containing personal information should not be sent to or received at a work email addresses (other than LCSB work email addresses) as this might be accessed by third parties.

8.5 The 'bcc' rather than the 'cc' or 'to' fields should be used when emailing a large number of people, unless everyone has agreed for their details to be shared amongst the group.

8.6 If personal devices have an LCSB account linked to them these should not be accessed on a shared device for which someone else has the pin code.

8.7 Personal data should be encrypted or password-protected before being transferred electronically.

8.8 Personal data should never be transferred **internationally** except in compliance with the law.

9. Sharing personal data

9.1 We will only share someone's personal data where we have a legal basis to do so, including for our legitimate interests within the LCSB (for example LCSB events held with other organisations). This may require information relating to criminal proceedings or offences or allegations of offences to be processed for the protection of children or adults who may be at risk and to be shared with Safeguarding Services or with statutory agencies.

10. How to deal with data security breaches

10.1 Should a data security breach occur, notification must be sent to the LCSB Data Protection Officer, Chair of Trustees and Leader of the community. If the breach is likely to result in a risk to the rights and freedoms of individuals, then the Information Commissioner's Office must be notified within 72 hours of the breach occurring. In the event of any data protection breach, consideration must be given by the Data Protection Officer, Chair of Trustees and Leader to notify the LCSB insurer within one week of the data protection breach.

10.2 Breaches will be handled by the Data Protection Officer.

11. Subject access requests

11.1 Data subjects can make a subject access request to find out what information is held about them. This request must be made in writing. Any such request received by the LCSB should be forwarded immediately to the LCSB Data Protection Officer who will coordinate a response within the necessary time limit (30 days).

11.2 It is a criminal offence to conceal or destroy personal data which is part of a subject access request.

12. Data subject rights

12.1 Data subjects have certain other rights under the UK GDPR. This includes the right to know what personal data the LCSB processes, how it does so and what is the legal basis for doing so.

12.2 Data subjects also have the right to request that the LCSB corrects any inaccuracies in their personal data, and erase their personal data where we are not entitled by law to process it or it is no longer necessary to process it for the purpose for which it was collected. Data should be erased when an individual revokes their consent (and consent is the basis for processing); when the purpose for which the data was collected is complete; or when compelled by law.

12.3 All requests to have personal data corrected or erased should be passed to the LCSB's Data Protection Officer who will be responsible for responding to them in liaison with the Trustees.

13 Contracts

13.1 If any processing of personal data is to be outsourced from the LCSB, we will ensure that the mandatory processing provisions imposed by the UK GDPR will be included in the agreement or contract.

14 Policy review

The LCSB Council and Data Protection Officer will be responsible for reviewing this policy from time to time and updating the LCSB in relation to its data protection responsibilities and any risks in relation to the processing of data.

Cycle of review – every 3 yrs	Last review	Next review
	June 2021	June 2024
Owner	Data Protection Officer	

Annex 1 Data Protection Notice

Data protection notice

Data controller: The Lay Community of Saint Benedict (LCSB) is registered as a data controller under the Data Protection Act 2018.

Personal data: Personal data about LCSB's members and friends and their families and other contacts are maintained by or for LCSB in paper-based filing systems and computerised databases, including LCSB's website (currently hosted by Netwise Hosting Ltd). The data are used for the purposes of LCSB, including communicating with members and friends and providing them with information which is thought likely to be of interest about the activities of LCSB and other bodies and persons. It is not LCSB's policy to pass personal data to other organisations without the express or implied consent of the person concerned.

Hard copy address list: A hard copy of LCSB's address list has been (and may continue to be) periodically circulated, principally by post, to members and other contacts of LCSB. It includes the names, postal and email addresses, telephone numbers, occupations and family details of most members. It facilitates communication between those listed. Any member who would prefer any or all of his or her personal data to be excluded from future address lists should give written instructions to that effect to LCSB's administrator and/or membership secretary.

Online address list: An electronic version of the address list is (or will be) maintained on a section of the LCSB website that may be accessed (by means of user IDs and passwords) by LCSB's Council members, Trustees, membership secretary, administrator and other permitted officers. It is generally accessible in the same way by LCSB's members; but any member may give written instructions to the contrary to LCSB's administrator and/or membership secretary.

Consent: Each member or friend of LCSB who provides to LCSB personal data about himself or herself (or about family members) consents (and confirms that each such family member consents) to the data being processed as described above.