Lowes Barn Community Project CIO	Confidentiality, Data Protection and Sharing Information Policy Version: 1.0	Status: Approved Date: 14th May 2023 Effective Date: 15th May 2023

Confidentiality, Data Protection and Sharing Information Policy

Introduction

1.1. In order to ensure the safe and efficient management of the Merryoaks Community Hall managed by the Lowes Barn Community CIO (LBCP), the LBCP must collect certain types of data. This personal information must be collected and handled securely.

1.2. The Data Protection Act 1998 (DPA) and General Data Protection Regulations (GDPR) govern the use of information about people (personal data). Personal data can be held on computers, laptops and mobile devices, or in a manual file, and includes email, minutes of meetings, CCTV and photographs.

1.3. The CIO will remain the data controller for the information held. The Trustees, staff and volunteers are personally responsible for processing and using personal information in accordance with the DPA and GDPR. Trustees, staff and volunteers who have access to personal information will therefore be expected to read and comply with this policy.

Policy Statement

1.4. We are committed to a policy of protecting the rights and privacy of individuals. The purpose of this policy is to set out the LBCP's commitment and procedures for protecting personal data. Trustees regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those whom we deal with. We recognise the risks to individuals of identity theft and financial loss if personal data is lost or stolen.

1.5. The aim of this policy is to:

1.5.1. Comply with the law.

1.5.2. Follow good practice.

1.5.3. Protect staff, volunteers and other individuals.

1.5.4. Protect the organisation.

1.5.5. Respect individuals' rights.

1.5.6. Be open and honest with individuals whose data is held.

1.5.7. Provide training and support for personnel who handle personal data, so that they can act confidently and consistently.

Lowes Barn Community Project CIO	**Confidentiality, Data Protection and Sharing Information Policy Version: 1.0**	**Status: Approved Date: 14th May 2023 Effective Date: 15th May 2023**

1.6. The following are definitions of the terms used:

1.6.1. Data Controller – is the LBCP, represented by the Trustees who collectively decide what personal information the LBCP will hold and how it will be held or used.

1.6.2. Act means the Data Protection Act 1998 and General Data Protection Regulations - the legislation that requires responsible behaviour by those using personal information.

1.6.3. Data Protection Officer – the person responsible for ensuring that the LBCP follows its data protection policy and complies with the Act and Regulations.

1.6.4. Data Subject – the individual whose personal information is being held or processed by the LBCP, for example, a member of staff or hirer.

1.6.5. Subject Access Request (SAR) – individuals have the right to ask us what personal information we hold on them.

1.6.6. 'Explicit' consent – is a freely given, specific agreement by a Data Subject to the processing of personal information about her/him. Explicit consent is needed for processing special category data, known under the DPA as "sensitive data", which includes:

- Racial or ethnic origin of the data subject.
- Political opinions.
- Religious beliefs or other beliefs of a similar nature.
- Trade union membership.
- Physical or mental health condition.
- Sexual orientation.
- Criminal record.
- Proceedings for any offence committed or alleged to have been committed.

1.6.7. Information Commissioner's Office (ICO) - the ICO is the UK's representative and responsible for implementing and overseeing the Data Protection Act 1998 and General Data Protection Regulations.

Lowes Barn Community Project CIO	**Confidentiality, Data Protection and Sharing Information Policy Version: 1.0**	**Status: Approved Date: 14th May 2023 Effective Date: 15th May 2023**

1.6.8. Processing – means collecting, amending, handling, storing or disclosing personal information.

1.6.9. Personal data – is information about living individuals that enables them to be identified, for example; names, addresses, telephone numbers and email addresses. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers.

The Data Protection Act

1.7. This contains 8 principles for processing personal data with which we must comply.

1.7.1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.

1.7.2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

1.7.3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

1.7.4. Personal data shall be accurate and, where necessary, kept up to date.

1.7.5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

1.7.6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

1.7.7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

1.7.8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures

an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

1.8. The lawful basis for processing data is set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

1.8.1. Consent: the individual has given clear consent for you to process their personal data for a specific purpose

1.8.2. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

1.8.3. Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations)

1.8.4. Vital interests: the processing is necessary to protect someone's life.

1.8.5. Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

1.8.6. Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks).

Applying the Data Protection Act within the LBCP

1.9. The LBCP will let people know why it is collecting their data, which is for the purpose of management of the LBCP, including Merryoaks Community Hall, its staffing (including volunteers) and finances. It is our responsibility to ensure the data is only used for this purpose. Access to personal information will be limited to authorised Trustees, staff and volunteers.

Purpose of data held by the LBCP

1.10. Data may be held by us for the following purposes:

- Staff Administration.

- Fundraising.
- Realising the Objectives of the LBCP.
- Accounts & Records.
- Advertising, Marketing & Public Relations.
- Information and Databank Administration.
- Journalism and Media.
- Processing For Not For Profit Organisations.
- Research.

- Management of Volunteers.

Responsibility

1.11. The LBCP is the Data Controller under the Act, and is legally responsible for complying with Act, which means that it determines what purposes personal information held will be used for.

1.12. The Trustees of the LBCP will take into account legal requirements and ensure that it is properly implemented, and through appropriate management, strict application of criteria and controls will:

1.12.1. Collect and use information fairly.

1.12.2. Specify the purposes for which information is used.

1.12.3. Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements.

1.12.4. Ensure the quality of information used.

1.12.5. Ensure the rights of people about whom information is held, can be exercised under the Act. These include:

- The right to be informed that processing is undertaken.
- The right of access to one's personal information.

- The right to prevent processing in certain circumstances.

- The right to correct, rectify, block or erase information which is regarded as wrong Information.

- Take appropriate technical and organisational security measures to safeguard personal information.

- Ensure that personal information is not transferred abroad without suitable safeguards.

- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information.

- Set out clear procedures for responding to requests for information.

1.13. All Trustees, staff and volunteers are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them.

Lowes Barn Community Project CIO	**Confidentiality, Data Protection and Sharing Information Policy Version: 1.0**	**Status: Approved Date: 14th May 2023 Effective Date: 15th May 2023**

The Data Protection Officer on behalf of the LBCP is:

- Name: Jennifer Thompson
- Telephone: 07713 242942
- Email: Chair@lowesbarncp.org.uk

1.14. The Data Protection Officer will be responsible for ensuring that the policy is implemented and will have overall responsibility for:

1.14.1. Briefing the Trustees, Staff and Volunteers on Data Protection responsibilities.

1.14.2. Reviewing Data Protection and related policies.

1.14.3. Everyone processing personal information understands that they are contractually responsible for following good Data Protection practice.

1.14.4. Ensuring that Data Protection induction and training takes place.

1.14.5. Anybody wanting to make enquiries about handling personal information knows what to do.

1.14.6. Dealing promptly and courteously with any enquiries about handling personal information.

1.14.7. Describe clearly how the charity handles personal information.

1.14.8. Will regularly review and audit the ways it holds, manages and uses personal information.

1.14.9. Will regularly assess and evaluate its methods and performance in relation to handling personal information.

1.14.10. Notification (Information Commissioners Office - ICO).

1.14.11. Oversee the handling of Subject Access Requests (SAR).

1.15. The Data Protection Officer is responsible for ensuring policies and procedures relating to personal and sensitive data, handled in the course of work, are shared with all staff and volunteers.

1.16. All information relating to data protection will be cascaded to staff and volunteers during the induction process to ensure that good data protection practice is established and followed. Staff and volunteers will be trained in their responsibilities, which will include whether information should be disclosed, or access allowed.

1.17. Trustees, staff, and volunteers must ensure that the Data Protection Officer is informed of any changes in their uses of personal data that might affect the LBCP's Notification (ICO).

Procedures for Handling Data & Data Security

1.18. The LBCP has a duty to ensure that appropriate technical and organisational measures and training are taken to prevent:

1.18.1. Unauthorised or unlawful processing of personal data.

1.18.2. Unauthorised disclosure of personal data.

1.18.3. Accidental loss of personal data.

Key Risks

1.19. The main risks within the LBCP are in two key areas:

1.19.1. Information about individuals getting into the wrong hands, through poor security or inappropriate disclosure of information.

1.19.2. Individuals being harmed through data being inaccurate or insufficient.

1.20. All Trustees, staff and volunteers must therefore ensure that personal data is dealt with properly no matter how it is collected, recorded or used. This applies whether or not the information is held on paper, in a computer or recorded by some other means e.g. tablet or mobile phone.

1.21. Personal data relates to data of living individuals who can be identified from that data and use of that data could cause an individual damage or distress. This does not mean that mentioning someone's name in a document comprises personal data; however, combining various data elements such as a person's name and salary or religious beliefs etc. would be classed as personal data, and falls within the scope of the Act. It is therefore important that all staff consider any information (which is not otherwise in the public domain) that can be used to identify an individual as personal data and observe the guidance given below.

Data Breach

1.22. Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security. Data security breaches include both confirmed and suspected incidents and include an incident, event or action which may compromise the confidentiality, integrity or availability of systems or data, which may result in

harm to individual(s), reputational damage, detrimental effect on service provision, legislative noncompliance, and/or financial costs to the LBCP.

1.23. Staff need to report suspected data breaches as soon as they are identified.

1.24. The LBCP will consult with relevant staff to establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.

Privacy Notice and Consent

1.25. Privacy notices and consent forms will be stored by the Data Controller in a securely held electronic or paper file.

Operational Guidance

1.26. Email:

1.26.1. All Trustees, staff and volunteers should consider whether an email (both incoming and outgoing) will need to be kept as an official record. If the email needs to be retained it should be saved into the appropriate folder or printed and stored securely.

1.26.2. Remember, emails that contain personal information no longer required for operational use, should be deleted from the personal mailbox and any "deleted items" box.

1.27. Phone Calls:

1.27.1. Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions should be taken:

1.27.2. Personal information should not be given out over the telephone unless you have no doubts as to the caller's identity and the information requested is innocuous.

1.27.3. If you have any doubts, ask the caller to put their enquiry in writing.

1.27.4. If you receive a phone call asking for personal information to be checked or confirmed be aware that the call may come from someone impersonating someone with a right of access.

1.28. Laptops and Mobile Devices:

1.28.1. LBCP does not allow the storage of data containing personal information on laptops and mobile devices except for short periods (less than 24 hours) in specific circumstances, for example to capture

data containing personal information when no internet access is available.

1.28.2. Laptops and personal devices that hold data containing personal information must be protected with a suitable encryption algorithm e.g a password or equivalent.

1.28.3. Ensure your laptop and/or mobile device is locked (password protected

or equivalent) when left unattended, even for short periods of time.

1.28.4. When travelling in a car, make sure the laptop and/or mobile is out of sight, preferably in the boot.

1.28.5. If you have to leave your laptop in an unattended vehicle at any time, put it in the boot and ensure all doors are locked and any alarm set.

1.28.6. Never leave laptops or mobile devices in your vehicle overnight.

1.28.7. Do not leave laptops or mobile devices unattended in restaurants or bars, or any other venue.

1.28.8. When travelling on public transport, keep your laptop or mobile devices with you at all times, do not leave it in luggage racks or even on the floor alongside you.

1.29. Security and Storage:

1.29.1. LBCP does not permit the storage or processing of personal data on personal computers, laptops or mobile devices except for short periods (less than 24 hrs, see also 12.3.1).

1.29.2. LBCP have established a secure password (or equivalent) controlled access LBCP Google Drive (cloud based) managed by three LBCP Trustees (Admin). Specific limited access folders have been established on the Google Drive for the storage of electronic files (documents, databases, photos, scanned documents etc.) containing personal data.

1.29.3. Store only as little personal data as necessary on the LBCP Google Drive as required to meet the management needs of the LBCP; only keep those files that are essential. Personal data received or uploaded from a device or memory stick should be saved to the relevant file on the LBCP Google Drive. The personal data on the device e.g. mobile phone or memory stick should then be wiped and securely disposed of, including deleting data in the Trash/Deleted folder.

1.29.4. Always lock (password or equivalent protection) any personal computer or laptop or mobile device used to access the LBCP Google Drive when left unattended.

1.29.5. Always ensure a screen time-out is enabled on any personal computer, laptop or mobile device used to access the LBCP Google Drive so that the Google Drive is secure from unauthorised access if the computer, laptop or device is left unattended and to prevent accidental disclosure of personal data to an unauthorised person.

1.30. Passwords:

1.30.1. Do not use passwords that are easy to guess. All your passwords should contain both upper and lower-case letters and preferably contain some numbers and a special character. Ideally passwords should be 6 characters or more in length.

1.30.2. Protect your password (if used for access security) and follow the common sense rules for passwords:

- Do not give out your password.
- Do not write your password somewhere on your computer, laptop or mobile device.
- Do not keep it written on something stored in the computer, laptop or mobile device case.

1.31. Data Storage:

1.31.1. Personal data will be stored securely and will only be accessible to authorised Trustees, volunteers or staff.

1.31.2. Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately. For financial records this will be up to 7 years. For employee records see below. Archival material such as minutes and legal documents will be stored indefinitely. Other correspondence and emails will be disposed of when no longer required or when Trustees, staff or volunteers retire.

1.31.3. All personal data held for the organisation must be non-recoverable from any computer which has been passed on/sold to a third party.

1.32. CCTV (Closed Circuit Television):

1.32.1. Use of CCTV is covered both by Data Protection legislation and by the Protection of Freedoms Act (POFA) and the Human Rights Act 1998 and particular care is therefore required in the use, recording, storage

and access to recorded material. Separate procedures will be required. This is to ensure that the rights of individuals recorded by surveillance systems are protected and that the information can be used effectively for its intended purpose. This will be covered by a separate CCTV policy. For further information contact the Data Protection Officer.

1.33. Information Regarding Recruitment, Employees or Former Employees:

1.33.1. Information regarding an employee or a former employee will be kept indefinitely. If something occurs years later it might be necessary to refer back to a job application or other document to check what was disclosed earlier, in order that Trustees comply with their obligations e.g. regarding employment law, taxation, pensions or insurance.

1.33.2. Recruitment information gathered from applicants who were unsuccessful, will be held for a limited period of six months, until it is clear that the unsuccessful applicant will not be offered a position with the LBCP.

1.34. Accident File:

1.34.1. The LBCP accident book is kept locked in the Office of Merryoaks Community Hall. All Users will have access to blank forms which, when completed will be returned to the Health and Safety Officer in a secure manner (e.g. sealed in an envelope) for filing securely.

1.35. Data Subject Access Requests (SAR):

1.35.1. The Freedom of Information Act 2000 gives individuals the right to request access to information held by public authorities, including the LBCP. Individuals have a right to make a Subject Access Request (SAR) to find out whether the LBCP holds their personal data, where, what it is used for and to have data corrected if it is wrong, to prevent use which is causing them damage or distress, or to stop marketing information being sent to them. Any SAR must be dealt with within 30 days. Steps must first be taken to confirm the identity of the individual before providing information, requiring both photo identification e.g. passport and confirmation of address e.g. recent utility bill, bank or credit card statement.

1.35.2. The LBCP may occasionally need to share data with other agencies such as the local authority, funding bodies and other voluntary agencies in circumstances which are not in furtherance of the management of the LBCP. The circumstances where the law allows the LBCP to disclose data (including sensitive data) without the data subject's consent are:

- Carrying out a legal duty or as authorised by the Secretary of State Protecting vital interests of a Data Subject or other person
  e.g. child protection.

- The Data Subject has already made the information public.

- Conducting any legal proceedings, obtaining legal advice or defending any legal rights.

- Monitoring for equal opportunities purposes – i.e. race, disability or religion.

1.35.3. The LBCP regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

1.35.4. The LBCP aims to comply fully with its obligations under the Act and to ensure that the service it provides for those wishing to gain access to information is simple, efficient, and effective.

1.35.5. Staff authorised to handle requests will follow the "How to deal with a request for information: A step by Step guide" on the ICO website at: https://ico.org.uk/for-organisations/sme-web-hub/how-to-deal-with-a request-for-information-a-step-by-step-guide/ .

1.36. Risk Management:

1.36.1. The consequences of breaching Data Protection can cause harm or distress to service users if their information is released to inappropriate people, or they could be denied a service to which they are entitled. Trustees, staff and volunteers should be aware that they can be personally liable if they use customers' personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of the LBCP is not damaged through inappropriate or unauthorised access and sharing.

Records

1.37. Records are kept to maintain our organisation and include health and safety records, development plans, financial records, and employment records of staff, volunteers (including student volunteers).

1.37.1. The induction process for all staff, volunteers and personnel working within the Merryoaks Community Hall includes an awareness of the importance of confidentiality and requires all to sign an agreement to

keep data containing personal information confidential.

Lowes Barn Community Project CIO	**Confidentiality, Data Protection and Sharing Information Policy Version: 1.0**	**Status: Approved Date: 14th May 2023 Effective Date: 15th May 2023**

1.37.2. Failure to comply with this policy may result in disciplinary action including dismissal.

1.37.3. This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998 and the General Data Protection Regulations – 25 May 2018.

1.37.4. In case of any complaints, queries or questions in relation to this policy please contact the Data Protection Officer (see Section 7).

Revision History

Revision	Approval date	Reason for changed
1.0	14th May 2023	Initial version

Printed Name: Jennifer Thompson Signed:

Role: Chair LBCP Date:

Lowes Barn Community Project CIO	**Confidentiality, Data Protection and Sharing Information Policy Version: 1.0**	**Status: Approved Date: 14th May 2023 Effective Date: 15th May 2023**

Appendix 1

Data Protection – Seven Golden Rules

Our procedure is based on the seven golden rules for information sharing as set out in Information Sharing: Advice for Practitioners (HM Government): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1062969/Information_sharing_advice_practitioners_safeguarding_services.pdf

The seven golden rules to sharing information

1. Remember that the General Data Protection Regulation (GDPR), Data Protection Act 2018 and human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.

2. Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. Seek advice from other practitioners, or your information governance lead, if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.

4. Where possible, share information with consent, and where possible, respect the wishes of those who do not consent to having their information shared. Under the GDPR and Data Protection Act 2018 you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear of the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared.

5. Consider safety and well-being: base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.

6. Necessary, proportionate, relevant, adequate, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles).

7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.