Bedfordshire & Luton Community Foundation

Policy Title	Data Protection Policy
Version	V4
Date Updated	Sept 23
Last Review Date	16/5/25
Next Review Date	May 2027

Data Protection Policy

1. Policy Statement

1.1 Bedfordshire and Luton Community Foundation (BLCF) is committed to a policy of protecting the rights and privacy of individuals, voluntary and community group members, volunteers, Trustees, staff, and others in accordance with the Data Protection Act 2018.

1.2 Any breach of The Data Protection Act 2018 or the BLCF Data Protection Policy is considered to be an offence, and in that event, disciplinary procedures apply.

1.3 As a matter of good practice, other organisations and individuals working with us, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that any staff who deal with external organisations will take responsibility for ensuring that such organisations sign a contract agreeing to abide by this policy.

1.4 BLCF is registered with the Information Commissioners Office.

2. Legal Requirements

2.1 Data are protected by the Data Protection Act 2018, which is the UK's implementation of the General Data Protection Regulation (GDPR).

2.2 Its purpose is to protect the rights and privacy of individuals and to ensure that personal data are not processed without their knowledge, and, wherever possible, not processed without their consent.

2.3 The Act requires us to acknowledge the right of 'subject access', this means that those about whom we hold data must have the right to copies of their own data. This includes staff, volunteers, and those for whom we hold data for fundraising or grant-giving purposes. This list is not exhaustive.

3. Managing Data Protection

3.1 We will ensure that our details are registered with the Information Commissioner should our operations require this. At present this is not the case. However, we still have responsibilities to safeguard the data that we hold.

3.2 BLCF further has a Website Privacy Policy to further cover data protection via our website www.blcf.org.uk and covered in our Website Privacy Policy.

3.3 All data held by BLCF on the organisations and individuals connected with the charities we fund is done so with the consent of the grantees awarded the funding.

3.4 All our funds require us to hold data on our Saleforce CRM system. Data collected is agreed in advance with the donor or funder and clearly communicated with groups applying for funding on the application form, website, and award letters.

3.5 Where required a fund programme will be supported by a Data Sharing Agreement with the relevant partner(s) or donors and that conforms to the requirements of the Foundations policy

3.6 Data collected and held may include the following.

- For individuals
  - Name, address, email and phone number
  - Financial data and personal evidence if rights to work
  - Relevant health information
  - Other specific information as and when required and by agreement.
- For charities and grantees and groups
  - Lean/main contact email, phone numbers and address
  - Address of charity or group or building associated
  - Details of finance and governance
  - Copies of key policies
  - Details of projects which have received funding.
  - Data and information of work delivered and beneficiaries of that work
  - Other specific information as and when required and by agreement.

4. Purpose of data held by Bedfordshire and Luton Community Foundation

4.1 Data may be held by us for the following purposes:

- Staff Administration
- Fundraising
- Reporting to donors
- Impact and evidence gathering.
- Evaluation of work strands
- Realising the Objectives of a Charitable Organisation or Voluntary Body
- Accounts & Records
- Advertising, Marketing & Public Relations
- Information and Databank Administration
- Journalism and Media
- Processing for Not for Profit Organisations
- Research
- Volunteers

5. Data Protection Principles

5.1 In terms of the Data Protection Act 2018, we are the ‘data controller’, and as such determine the purpose for which, and the manner in which, any personal data are, or are to be, processed. We must ensure that we:

5.2 Have a Lawful Basis for Processing Data

5.2.1 Under regulations, data can only be processed if there is at least one lawful basis to do so. The lawful bases for processing data are:

- Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
- 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.
- Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- Vital interests: the processing is necessary to protect someone's life.
- 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.
- 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.)

5.3 Identify Processes and Privacy

5.3.1 We will always put our logo on all paperwork that gathers information, and on electronic means, stating their intentions on processing the data and state if, and to whom, we intend to give the personal data. We will also provide an indication of the duration the data will be kept.

5.4 Processed for limited purpose.

5.4.1 We will not use data for a purpose other than those agreed by data subjects (donors, funders, associates, staff, and others). If the data held by us are requested by external organisations (not those listed) for any reason, this will only be passed if data subjects (donors, funders, associates, staff, and others) agree. Also, external organisations must state the purpose of processing, agree not to copy the data for further use and sign a contract agreeing to abide by The Data Protection Act 2018 and BLCF's Data Protection Policy.

5.5 Adequate, relevant, and not excessive

5.5.1 BLCF will monitor the data held for our purposes, ensuring we hold neither too much nor too little data in respect of the individuals about whom the data are held. If data given or obtained are excessive for such purpose, they will be immediately deleted or destroyed.

5.6 Accurate and up to date

5.6.1 We will provide relevant persons including staff and volunteers with a copy of their data once a year for information and updating where relevant. All amendments will be made immediately, and data no longer required will be deleted or destroyed. It is the responsibility of individuals and organisations to ensure the data held by us are accurate and up to date. Completion of an

appropriate form (provided by us) will be taken as an indication that the data contained are accurate. Individuals should notify us of any changes, to enable personnel records to be updated accordingly. It is the responsibility of BLCF to act upon notification of changes to data, amending them where relevant.

5.7 Not kept longer than necessary

5.7.1 We discourage the retention of data for longer than it is required. All personal data will be deleted or destroyed by us according to contractual and legal requirements.

5.8 Processed in accordance with the individual's rights

5.8.1 All individuals that BLCF holds data on have the right to:

- Be informed upon the request of all the information held about them within 40 days.
- Prevent the processing of their data for the purpose of direct marketing.
- Compensation if they can show that they have been caused damage by any contravention of the Act.
- The removal and correction of any inaccurate data about them.

5.9 Secure

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

5.9.2 All BLCF computers have a log in system and our Contact Database is password protected, which allow only authorised staff to access personal data. Passwords on all computers are changed frequently. All paper-based personal and financial data is kept in a locked filing cabinet and can only be accessed by the Executive officers. When staff members are using the laptop computers out of the office care should always be taken to ensure that personal data on screen is not visible to strangers.

5.10 Complies with UK GDPR regulation and Data Subject Rights which are:

5.10.1 Right to be informed

5.10.2 Right of access

5.10.3 Right to rectification

5.10.4 Right to erasure

5.10.5 Right to restrict processing

5.10.6 Right to data portability

5.10.7 Right to object

5.10.8 Rights in relation to automated decision-making

5.11 Not transferred to countries outside the European Economic Area, unless the country has adequate protection for the individual.

5.11.1 Data must not be transferred to countries outside the European Economic Area without the explicit consent of the individual. BLCF takes particular care to be aware of this when publishing information on the Internet, which can be

accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the European Economic Area.

6. Documentation of the data held by BLCF

6.1 'Personal data' under the GDPR means any information relating to an identified or identifiable natural person who can be directly or indirectly identified, by reference to an identifier such as a name, identification number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

6.2 As required by Data Protection Act 2018, we document the personal data we hold, where we obtained the information and who we may share it with (if anyone). It forms our Data Protection Register.

7. Training

7.1 All members of staff and volunteers are provided with training on Data Protection compliance on induction and as necessary from time to time. Additional training on any changes to this policy and refresher training will be provided annually.

7.2 Any member of our staff or volunteer with an enquiry about the handling and processing of personal data should approach the named individual who is responsible for data protection in BLCF.

7.3 Each staff member and volunteer is responsible for ensuring that no breaches of this policy result from their actions. Failure to comply with this policy by any member of staff may result in disciplinary proceedings.

8. Data breaches

8.1.1 Each staff member and volunteer have a responsibility towards any breaches of data. Should a staff member become aware of a potential or actual data security breach they MUST notify the CEO immediately. The most common causes of data breaches include:

- Letters or emails being addressed to and sent to the wrong recipient.
- Files or papers being lost (whether in the office of when removed from the office)
- An individual inadvertently seeing or reading information about another individual or organisation when visiting the office.
- Loss of memory sticks (or other removable media)
- Loss of, or theft of laptops or devices containing personal data relating to grantees or staff
- Potential loss where our firewall and anti-viral software is breached due to computer viruses, malware, or ransomware.

8.1.2 Under the GDPR, the Data Controller is under a legal obligation to consider notifying the ICO if the breach could affect the rights and freedoms of the individuals concerned.

9. Passing data to third parties

9.1 In the context of providing services or managing staff contracts, it may be necessary to instruct and pass data to a third-party. Some of them will also be data controllers under the legislation and be required to operate the same standards that we do. Others will be data processors, simply processing data on BLCF's behalf, for example: IT Providers Contact Management System Providers, Cloud Storage Providers, IT Support Companies, Online Services including MailChimp, SurveyMonkey), file storage or destruction companies, external payroll companies.

9.2 Whenever we instruct a data processor and pass confidential data to them, the legislation requires that we have a written agreement in place.

9.3 Data regarding grants management and awards may be shared with funders and donors in line with the policy and agreement of the grantees. Funders and donors must agree the level of data required at the start of any agreement and they must comply with this policy and Data Protection Act 2018.

9.3.1 A funder/donor may request a supplemental data sharing agreement. This must not be in conflict with the foundations own data protection (this) policy.

9.3.2 Request for data must be proportionate and agreed by any grantees as part of the application process and grant award letter.

9.3.3 This data protection policy takes precedence over any supplemental agreement.

-END-

Version Change Information

1. Rewritten to incorporate Data Protection Act 2018 requirements and information from Staff Handbook