Policy Title	JCT Data Protection Policy
Version	V1.0
Approved	20th Nov 2025
Last Review Date	20th Nov 2025
Next Review Date	Nov 2028

The Mrs Jane Cart Trusts
Data Protection Policy

Policy Statement

- The Mrs Jane Cart Trusts (JCT), and Bedfordshire and Luton Community Foundation (BLCF) who transact their business, are committed to a policy of protecting the rights and privacy of individuals, voluntary and community group members, Trustees, and others in accordance with the Data Protection Act 2018.
- Any breach of The Data Protection Act 2018 or the BLCF Data Protection Policy is an offence, and in that event, disciplinary procedures will apply.
- As a matter of good practice, other organisations and individuals working with BLCF, 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
- JCT is registered with the Information Commissioners Office.

Legal Requirements

- Data is protected by the Data Protection Act 2018, which is the UK's implementation of the General Data Protection Regulation (GDPR).
- Its purpose is to protect the rights and privacy of individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, not processed without their consent.
- The Act requires JCT and BLCF to acknowledge the right of 'subject access', this means that those about whom they hold data must have the right to copies of their own data. This includes staff, volunteers, and those for whom data is held for fundraising or grant-giving purposes. This list is not exhaustive.

Managing Data Protection

- JCT manages all data through its service contract with Bedfordshire and Luton Community Foundation (BLCF). As such all data management on behalf of JCT is managed by BLCF, including data on grantees, individual applicants, Trustees and others.
- BLCF ensures that its details are registered with the Information Commissioner should their operations require this. At present this is not the case. However, they still have responsibilities to safeguard the data held.

- JCT grant applications are made via the BLCF website. The BLCF website also has a Website Privacy Policy to further cover data protection via their website www.blcf.org.uk
- All data collected and held by BLCF on the organisations, and individuals connected with the charities that JCT fund, is done so with the consent of the applicants. JCT data is held on a secure SharePoint System managed by BLCF and accessed by authorised staff using Multi-Factor Authentication and LastPass password protection systems.
- BLCF's own activities require them to hold data on their Salesforce 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.
- 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
        - Name/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.

Purpose of data held by Bedfordshire and Luton Community Foundation

- Data may be held for the following purposes:

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

Data Protection Principles

- In terms of the Data Protection Act 2018, BLCF are the 'data controller' for JCT, and as such determine the purpose for which, and the way, any personal data is to be processed. It is important to ensure that:

There is a Lawful Basis for Processing Data

- 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 their personal data to be processed for a specific purpose.
  - Contract: the processing is necessary for a contract with the individual, or because they have asked for specific steps to be taken before entering a contract.
  - Legal obligation: processing is necessary to comply with the law (not including contractual obligations).
  - Vital interests: processing is necessary to protect someone's life.
  - Public task: the processing is necessary to perform a task in public interest or for an official function, and the task or function has a clear basis in law.
  - Legitimate interests: processing is necessary for 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 for a public authority processing data to perform an official task.)

Identify Processes and Privacy

- BLCF will always put JCT logo on all paperwork that gathers information, and on electronic means, stating their intentions for processing the data and state if, and to whom, it is intended to give the personal data. An indication of the duration for which the data will be kept will be provided.

Processed for limited purpose

- BLCF will not use data for a purpose other than those agreed by data subjects (donors, funders, associates, staff, and others). If the data held is 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 JCT's Data Protection Policy.

Adequate, relevant, and not excessive

- BLCF will monitor the data held for JCT purposes, ensuring it is neither too much nor too little data in respect of the individuals about whom the data is held. If data given or obtained is excessive for such purpose, it will be immediately deleted or destroyed.

Accurate and up to date

- BLCF will provide relevant people including Trustees, 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 the JCTs is accurate and up to date. Completion of an appropriate form (provided by BLCF) will be taken as an indication that the data contained is accurate. Individuals should notify BLCF 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.

Not kept longer than necessary

- BLCF discourages the retention of data for longer than is required. All personal data which is held will be deleted or destroyed according to contractual and legal requirements.

Processed in accordance with the individual's rights

- All individuals whose data is held by BLCF have the right to:
    - Be informed upon 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 damaged by any contravention of the Act.
    - The removal and correction of any inaccurate data about them.

Secure

- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.
- All JCT data is held on BLCF computers which have a log in system and the Contact Database is password protected, which allows only authorised staff to access personal data. Passwords on all computers are changed frequently.
- When BLCF staff are using the laptop computers out of the office, care will be taken to ensure that personal data on screen is not visible to strangers.
- All paper-based personal and financial data is kept in a locked filing cabinet and can only be accessed by the Executive Officer.
- All data shared with Trustees for the purpose of Grants Committee discussions is done so through a shared and secured **Drop Box**. The Drop Box is password protected and only accessible to authorised staff at BLCF and JCT Trustees. All Drop Box data is deleted after decisions are made regarding grant allocations

- Data is shared with Trustees by email only by exception. When it is, Trustees are requested to delete emails once Trustees have dealt with the query and are advised not to store personal data on home laptops for any reason.

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

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights in relation to automated decision-making

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

- Data must not be transferred to countries outside the European Economic Area without the explicit consent of the individual. BLCF and JCT take 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.

Documentation of the data held by BLCF

- '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.
- As required by Data Protection Act 2018, personal data held is documented, from where it was obtained and with whom it may be shared (if anyone). It forms the Data Protection Register.

Training

- All members of BLCF staff managing data 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.
- Any member of BLCF staff with an enquiry about the handling and processing of personal data should approach the named individual who is responsible for data protection in BLCF.
- 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.

Data breaches

- Each BLCF staff member has 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 sees or reads information about another individual or organisation when visiting the office.
- Loss of memory sticks (or other removable media)
- Loss, or theft, of laptops or devices containing personal data relating to grantees or staff
- Potential loss following the breaching of the firewall and anti-viral software due to computer viruses, malware, or ransomware.

- Any query regarding data storage or handling raised with BLCF is reported to JCT Trustees.
- 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.

Passing data to third parties

- 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 BLCF do. Others will be data processors, simply processing data on JCTs or BLCFs 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.
- Whenever instructions are given to a data processor and confidential data is passed to them, the legislation requires that we have a written agreement in place.

-END-

Version Change Information

1. Rewritten to incorporate Data Protection Act 2018 requirements