The Hub
LITTLE PAXTON
2 Samuel Jones Crescent, Little Paxton PE19 6QY
Registered Charity Number 1173213

Confidentiality, Data Protection and Security Policy[1]

THE COMMUNITY HUB LITTLE PAXTON CHARITABLE INCORPORATED ORGANISATION (hereinafter referred to as "THE ORGANISATION") is bound by the Data Protection Act 1998 and any subsequent updates. This protects personal data and restricts an Organisation's ability to disclose personal data. Personal data is information relating to an individual from where he/she can be identified *e.g. name, address, tax details or national insurance number*.

Trustees, staff and volunteers of **THE ORGANISATION** may be given personal/business information in confidence by –

- an individual;
- a service user *e.g. hirers or contractors;*
- group(s) of service users; or
- Trustee(s) in connection with the management of **THE ORGANISATION**.

Anyone working for or associated with **THE ORGANISATION** has a duty to protect the confidentiality of personal/business information and to process or exchange personal/business information with the correct safeguards.

1. Data Protection Act 1998

The Data Protection Act 1998 regulates when and how an individual's personal data may be obtained, held, used, disclosed and processed. It applies to computerised processing of personal data and paper based files and records held in a relevant filing system.

To comply with the law, information must be collected and used fairly, stored securely and not disclosed to any other person unlawfully. To do this **THE ORGANISATION** must comply with the Data Protection Principles, which are set out in the Data Protection Act. These state that personal data must be -

- obtained and processed fairly and lawfully;
- up to date, adequate, relevant to specific purpose(s) and not excessive;
- kept secure, marked in the appropriate manner *e.g. Confidential*[2] *or Sensitive*[3] and protected;
- kept no longer than necessary; and
- the subject of the personal information will be allowed to view such data upon request *(see Item 2 post).*

2. Requests for Access to Data Held

An individual may have sight/copy of records held in his/her name by **THE ORGANISATION.**

To ensure that such a request is genuine, an email or form should be sent to the person for completion. If a third party is acting on behalf of the individual, proof of the third party's identity and the individual's authority to disclose his/her information to their representative, must be obtained in writing. All requests must be responded to within 20 working days. They are entitled to see –

---

[1] The information you provide *(such as name, address, email address, phone number, organisation, etc)* will be processed and stored so that it is possible to contact you and respond to your correspondence, provide information and/or access The Hub's facilities. Your personal information will not be shared or provided to any other third party.

[2] Confidential files should state the name of the individual.

[3] Sensitive information *e.g. disputes or legal issues* is confidential to the Trustee(s), staff member(s) and volunteer(s) dealing with the issue(s).

- a description of the personal data;
- the purpose(s) for which they are being processed; and
- the disclosures, or potential disclosures, of the personal data.

3. Data Controller Status

THE ORGANISATION retains personal information for the Organisation's use so the legal duty to register with the Information Commissioner's Office as a Data Controller will be complied with.

4. Telephone/Email Support

(a) **THE ORGANISATION** telephone support is bound by this confidentiality policy.

(i) The Telephone Support Worker will state the following statement about confidentiality during the course of each telephone call -

"The information you give me will be dealt with confidentiality. However if you want family assistance, we will need your agreement to pass some of your personal details to Organisations that may be able to help you."

(ii) Many of the calls that **THE ORGANISATION** handle will involve discussion of the caller's personal information and circumstances, in particular health and financial matters.

When undertaking such services on behalf of callers, Telephone Support Workers should

- remind the caller of the confidential nature of the Service and that his/her agreement to the sharing of this information may be needed in order to apply for additional support or grants on their behalf;
- make it clear to the caller which Organisation the information will be sent to; and
- ensure a copy of any such correspondence/email is sent to the caller.

(b) Any Support Service email should conclude with the following sentence -

"The Community Hub Little Paxton Charitable Incorporated Organisation support services are confidential and secure. However if you want external family assistance, we will need your agreement to pass some of your personal details to Organisations that may be able to help you. "

There are certain other circumstances in which confidentiality may need to be broken. These are outlined in this policy under 'Breaking Confidentiality' *(see Item No. 5 post)* together with the procedures that Support Workers should follow.

5. Breaking Confidentiality /Information about a Crime

(a) Confidentiality may be broken in the following circumstances –

- where the person from whom the information was obtained, and *(if different)* the person to whom it relates, consents;
- where the information is already available to the public from other sources;
- where the information is in the form of a summary or collection of information so framed that it is not possible to ascertain from its contents it relates to any particular person;
- when there is a serious risk of harm to the individual, as in a threatened suicide;
- to protect others e.g. information about possible child abuse should be disclosed to the appropriate agency. See the Safeguarding Policy; and
- to prevent a serious criminal act, especially where others may be endangered, for example an act of terrorism.

(b) It is a criminal offence to –

- deliberately mislead the Police;
- fail to notify the Police about an act that could be construed as an act of terrorism;
- fail to notify the Police about an act that could be construed as drug trafficking;
- knowingly take monies from a Benefits Agency fraudulently; and
- receive a reward of any kind in return for not notifying the Police about a criminal act;

If **THE ORGANISATION** has to break confidentiality, or consider breaking it, the individual whose personal information is to be disclosed must be informed either verbally or in writing. This should only be done after all attempts to persuade the individual to disclose the information voluntarily have failed. The Chief Officer of the appropriate Group(s) and Chairperson of **THE ORGANISATION** must be consulted and authorise such action.

6. Handling Complaints

If a member of the public expresses concern about his/her 'information rights' practices, **THE ORGANISATION** is responsible for dealing with the matter.

THE ORGANISATION will respond to any 'information rights' concerns received. Clarification will be sought/given to the complaint as to how the individual's personal information was processed and he/she informed of any resultant remedial action to be implemented.

If a member of the public has engaged with **THE ORGANISATION** but is still dissatisfied, they may refer their concern(s) to the Information Commissioner's Office *(website: http://www.ico.org.uk/).*

7. Data Protection/Security

THE ORGANISATION commits to take the following security measures to protect data in its care –

(a) Computers, etc

- Install firewall/virus-checking/anti-spyware software on computer/tablets, etc. used/belonging **to THE ORGANISATION.**
- Protect **THE ORGANISATION** computers, etc. by setting operating system(s) to receive automatic updates or downloading the latest patches or security updates,
- Only allow nominated Trustees, staff and volunteers of **THE ORGANISATION** access to software/information required to undertake their duties.
- Encrypt any personal information held electronically that could cause damage or distress if lost or stolen.
- Take regular back-ups of information held on **THE ORGANISATION** computer systems and store in a designated secure area.
- Securely remove all personal information before disposing of old computers e.g. *by using technology or destroying the hard disk.*

(a) Email

- Consider whether the content of an email(s) should be encrypted or password protected.
- Ensure emails are sent to the right addresses.
- Use blind carbon copy (*bcc)* on group emails to protect the recipients from obtaining other email addresses.
- Check that the recipient's arrangements are secure before sending email messages when necessary.

(b) Fax

- Consider whether using email or courier may be more secure than fax.
- Check before sending a fax to a recipient that adequate security is in place
- Check the fax number(s). Dial from a directory of previously verified numbers.
- If the fax is sensitive, ask the recipient to confirm that they are at the fax machine, they are ready to receive the document and there is sufficient paper in the machine.
- Telephone or email the recipient to confirm that the whole document has been received safely.
- Use a cover sheet to ensure the intended recipient is immediately aware that the information is confidential/sensitive without the need to review its contents.

(c) Security

Ensure Trustees, staff and volunteers –

- use a strong password *(at least seven characters, containing a combination of upper and lower case letters, numbers and special keyboard characters e.g. asterisk or currency symbols)* and not shared*;*
- are aware of spam emails/people trying to obtain personal details *e.g. passwords, bank/credit card details*;
- do not bring **THE ORGANISATION**/Groups into disrepute by sending offensive emails;
- are aware prosecution can result if they deliberately give out personal details without permission;
- shred all confidential paper waste; and
- check the physical security of premises.

8. Data Sharing

In order to provide the most effective support package for service users, there may be times when it is necessary to share users' personal information with other Organisations. Any requests for information made to **THE ORGANISATION** through an Organisation/Group will be obtained in writing and data will only be provided after the service user has consented to the data being collected and in accordance with the individual Organisation's Data Protection, Confidentiality and Privacy Policies.

9. Publication

The fact that some services undertaken by **THE ORGANISATION** are confidential and secure will be stated in all social media, websites, emails and other publicity/information materials. **THE ORGANISATION** will display its Registered Charity Number on all publications and accurately use, after consultation, the logo of their funders.

10. Disclosure and Barring Service

Data received through Disclosure and Barring Service Checks will be stored, handled and secured appropriately in line with the Disclosure and Barring Service Code of Conduct.

11. Training

THE ORGANISATION will induct Trustees, staff and volunteers in the importance of data protection and confidentiality, maintain on-going reminders and use the ICO Think Privacy Toolkit to raise awareness of the issue in its premises.

12. Monitoring and Review

The Board of Trustees will regularly review the operation of this policy.

✂ ----------

Please complete *(in block capitals),* sign and return

THE HUB LITTLE PAXTON
Samuel Jones Crescent, Little Paxton, St Neots, PE19 6BL

Confidentiality, Data Protection and Security Policy
(Adopted: October 2023)

I, …… have duly read and fully understand the above Policy and will comply with its contents.

Signed: …….. Position: …….

Date: ……..

Due for review: October 2024