Information Security Policy (GDPR)

POLICY STATEMENT

All staff and volunteers of CHIPS shall always follow the procedures laid out in this policy regarding access and use of any personal information held, stored or processed by CHIPS.

Information is vitally important to CHIPS and we all have a responsibility to make sure that this information is kept safe and used appropriately. Without due care, business or personal information can be misplaced or leaked; as well as attempts at theft or a cyber-attack.

CHIPS has adopted an 'Information Security Policy' that complies with the legal requirements (General Data Protection Regulation 2018) and provides the necessary assurance that data held and processed by CHIPS, is treated with the highest standards to keep it safe.

This policy sets out the responsibilities and required behaviour for users of the Charities information systems, networks and computers; and the personal information held within.

All staff, volunteers, trustees and persons whom have been granted access to use CHIPS facilities are subject to this policy.

This Information Security Policy (includes Mobile Data, Disposal, Breach and systems Management)

SECTION 2
POLICY PROCEDURES

General Procedures
All staff ,volunteers and trustees must consider and adhere to the following procedures, on the safe use, storage and access to information held by CHIPS.

Information Collection
All personal information must only be collected and stored, if a legitimate interest or legal requirement is present, or consent is given by the data subject.

Much of the personal information held is done so as a Legitimate Interest. Over the course of the next year 'Consent' will be sought from the data subjects. Any consent given to hold personal information; will consent to CHIPS holding their information for a period of 5 years.

Basis for Collecting and Storing Information
CHIPS information as a 'Data Controller' in a number of ways, including:

- As an organisation trustees and volunteers.
- As a provider of personalised services to beneficiaries and clients.
- As a fundraising or campaigning organisation that has donors and supporters.

CHIPS will also process information as a 'Data Processor', managing its own data processing systems. Such as:

- Shredding documents containing personal data
- Posting
- Putting a photo of a person on a website
- Storing IP addresses
- Video recording

Audit of Personal Information
A current and accurate record of personal information held about data subjects, can be found in the CHIPS GDPR database', which provides, an overview of all personal information held within the Charity.

The database specifies who has access to the information, for what specified purpose it was collected, who it was collected by, how & where it is stored and when the information is due to be deleted.

This information will be maintained accurately and up to date.

Access to Personal Information
All computers, mobile devices and phones must be password protected.

Only the staff, volunteers and trustees who require the use of the device will be provided with the password.

CHIPS will use a secure 'cloud' to save and back up all information. Access to information is restricted and only available, on a need to know basis.

Information is restricted on a need to know basis, with specific staff, volunteers, trustees invited to view folders.
All personal information is saved using initials only to reduce identification/breach possibilities.

A system of saving information has been implemented across the organisation, to ensure –

- that all staff, volunteers and trustees are saving information securely
- that it is known where the information has been saved
- it is known who has access to that information
- the information can be clearly tracked, monitored and deleted at the appropriate time.

Information Sharing

Any information being shared with a third party, must be done so in compliance with GDPR legislation.

For any client or contractor, whom we may share information with; an 'Information Sharing Agreement' must be in place, specifying the manner in which the information will be used; where it will be stored; who will have access and when it will be deleted.

Any information being shared with a third party will ideally be transferred electronically, via a secure or encrypted method (encrypted USB or shared cloud folder).

Where possible information must be anonymised, using initials rather than names. Only specifically requested information must be shared, do not just share everything held on that person.

If sharing information, ensure consent to share is provided, and confirm the ID of the person requesting the information, before releasing it.

All Information Sharing Agreements are recorded on the GDPR Database.

Disposal or Removal of Information

A Data Subject has rights under the GDPR legislation; they have the right to -

- Access, rectify or update their information
- Delete their information

- Ask for their information to be transferred (data portability) to another organisation

Data is held by CHIPS for a specified period of time, depending upon the reason for collecting / holding it. Once the personal information is no longer required, it must be destroyed in a safe and secure manner. The methods of disposal will be recorded on the GDPR database.

Breach - Reporting Losses

Any personal information lost stolen, missing, left behind, or accessed by any unauthorised persons; must be reported. Any significant risk to an individual will be taken seriously, possibly reported to the ICO as a 'Data Breach'.