Tel No: 07720 206532
Email: enquiries@thecoddenhamcentre.co.uk
Registered Charity No : 1183244

THE CODDENHAM CENTRE

The Coddenham Centre

Data Protection Policy

(GDPR Compliant)

Introduction

This Policy applies to the processing of personal data in manual and electronic records kept by the Coddenham Centre Charitable Incorporated Organisation (CIO) in connection with its functions as described below. It also covers the CIOs response to any data breach and other rights under the General Data Protection Regulation.

This Policy sets out how we seek to protect personal data and ensure that Trustees and Staff of the Coddenham Centre understand the rules governing their use of personal data to which they have access to in the course of their work. In particular, this Policy requires CIO to ensure that the Data Protection Controller be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

We hold personal data about our employees, residents, suppliers and other individuals for a variety of purposes.

Definitions

"Business/ purposes"	The purposes for which personal data may be used by us: Personnel, administrative, financial, statutory and legislative purposes, payroll, consultations and business development purposes. *CIO purposes include the following:* - *Compliance with our legal, regulatory and corporate governance obligations and good practice* - *Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests* - *Ensuring CIO policies are adhered to (such as policies covering email and internet use)* - *Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of sensitive information, security vetting and checking* - *Investigating complaints* - *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments* - *Monitoring staff conduct, disciplinary matters* - *Promoting services* - *Improving services*

"Personal data"	Information relating to identifiable individuals, such as job applicants, current and former employees, clients, suppliers and marketing contacts, members of the public, Centre users, hirers, correspondents *Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV, contact details, correspondence, emails, databases*
"Sensitive personal data"	*Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.*
"Data Processing"	*Data processing is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*
"Criminal Offence date"	*Criminal Offence data is data which relates to an individual's criminal convictions and offences.*

The CIO make a commitment to ensuring that personal data, including sensitive personal data and criminal offence data (where appropriate) is processed in line with GDPR and domestic laws and that all its Trustees and staff conduct themselves in line with this, and other related policies. Where third parties process data on behalf of the CIO the CIO will ensure that the third party takes such measures in order to maintain the CIO's commitment to protecting data. In line with GDPR, the CIO understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

Data Protection Principle

All personal data obtained and held by the CIO will:

- be processed fairly, lawfully and in a transparent manner
- be collected for specific, explicit, and legitimate purposes
- be adequate, relevant and limited to what is necessary for the purpose of processing
- be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay
- not be kept for longer than is necessary for its given purpose
- be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
- comply with the relevant GDPR procedures for international transferring of personal data.

In addition, personal data will be processed in recognition of an individuals' data protection rights, as follows:

- the right to be informed
- the right of access
- the right for any inaccuracies to be corrected (rectification)
- the right to have information deleted (erasure)
- the right to restrict the processing of the data
- the right to portability
- the right to object to the inclusion of any information
- the right to regulate any automated decision-making and profiling of personal data.

Procedures

The CIO has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access:

- it can account for all personal data it holds, where it comes from, who it is shared with and also who it might be shared with
- it recognises the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their personal data, and regularly reviews its procedures for doing so. The CIO understands that consent must be freely given, specific, informed and unambiguous. The CIO will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time

Data Security

The CIO adopts procedures designed to maintain security of data when it is stored and transported. In addition, individuals must:

- ensure that files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them
- ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people
- check regularly on the accuracy of data being entered into computers
- always use passwords provided to access the computer system and not abuse them by passing them on to people who should not have them

Personal data relating to individauls should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by the Trust Chairman

.

Where personal data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where absolutely necessary
- using an encrypted system – a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted

- ensuring that laptops or USB drives are not left lying around where they can be stolen.

In cases where data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.

The Trust Secretary is the CIO's appointed compliance officer, data controller and data processor.

The CIO takes compliance with this policy very seriously. The policy will be reviewed annually.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the Trust Secretary.

Date approved or amended	**Signed**	**Position**
31st October 2019	Angela Thapson	Trust Secretary