Working for the mental well-being of young people

Data Protection Policy

Approved: Trustees 23rd January 2020.

Review due: By January 2022.

Purpose

This policy outlines the key requirements placed upon the Clockwork Charitable Trust by General Data Protection Regulation (GDPR), and data retention legislation, with regards to receiving, recording, organising, storing, protecting and destroying data concerning its service users, employees and volunteers.

Responsibilities and monitoring

Monitor: Data Protection Officer

Approve: Board of Trustees

Draft and review: Development Officer

Policy and Procedure

The Clockwork Charitable Trust will ensure it meets its legal responsibilities as outlined in the Data Protection Act (2018), commonly referred to as General Data Protection Regulation (GDPR).

The purpose of the GDPR is to protect an individual's rights and freedoms and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

The Clockwork Charitable Trust will abide by the GDPR principles of:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality.

Governance, Compliance and Accountability:

The Clockwork Charitable Trust is a data controller and data processor under the GDPR. The Trustees, Data Protection Officer (DPO) and members of staff are responsible for developing and encouraging good information handling practices within the organisation.

Compliance with data protection legislation is the responsibility of all trustees, members of staff and volunteers who process personal data as part of their work for the Trust. The DPO will have responsibility for overall supervision and ongoing compliance with data protection laws.

Trustees, employees and volunteers are responsible for ensuring that the personal data they provide to the Trust is, to the best of their knowledge, accurate and up-to-date.

Rights:

All service users, members of staff, potential employees and volunteers have the following rights concerning their data:

- **To be informed** about the collection and use of their personal data at the time it is collected, along with how it will be processed and who will have access to it;
- **To have access** to any personal information that the Trust holds about them;
- **To correct** any inaccurate information, or update their personal information;
- **To erase** personal data, in accordance with data protection laws, as well as to object to any direct marketing from the Trust, and to be informed about any automated decision making that is used;
- **To restrict** the processing of personal data. The Trust may still retain the data, in accordance with data protection laws, but not use it;
- **To portability** of personal data, allowing the individual to obtain and reuse their personal data for their own purposes across different services;
- **To object** to the processing of personal data.

If the Trust receives a request to exercise any of the above rights, verification of identity may be asked for before acting on the request; this is to ensure that data is kept protected and secure.

All requests to exercise rights will be given to the DPO, who will oversee all related investigations and resulting changes.

Privacy Notices:

A privacy notice outlines how, why and when we gather and process personal information in compliance with the relevant data protection regulation, as well as providing an outline of the necessary information regarding rights and obligations. The Clockwork Charitable Trust has the following privacy notices:

• Customer Privacy Notice – relating to users of Clockwork Charitable Trust services

• Staff Privacy Notice – relating to current and former employees and volunteers

• Recruitment Privacy Notice – relating to job applicants.

All privacy notices can be found at clockwork.org.uk

Documenting Lawful Basis:

When processing personal data, the Trust will always identify and establish the legal basis for doing so. This is determined by the purpose of processing the data and the relationship with the individual, and may include:

- Protecting the vital interests of a data subject e.g. providing medical information in an emergency;
- Legal obligation e.g. carrying out enhanced DBS checks on all members of staff and volunteers;
- Legitimate interests e.g. where people would expect us to process data, such as contact details of a service user.

Consent:

The Clockwork Charitable Trust understands consent to mean that it has been explicitly and freely given by statement or a clear affirmative action, signifying agreement to the processing of personal data.

In most instances, consent to process personal and sensitive data is obtained routinely using standard consent documents e.g. booking conditions for a service. For sensitive data, explicit written consent must be obtained, unless an alternative legitimate basis for processing exists.

Consent can be withdrawn at any time.

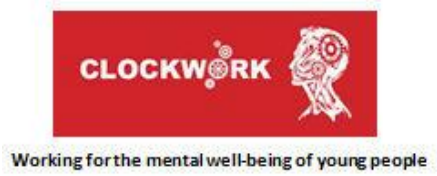
Data Breaches:

A personal data breach is defined as a security incident that has affected the confidentiality, integrity or availability of personal data. This might include personal data being lost, corrupted or being accessed by someone without the correct authorisation.

If a security incident takes place, the DPO must be informed immediately. The DPO should assess the immediacy and severity of the situation, and establish whether a personal data breach has occurred.

Where immediate action needs to be taken, the DPO will instruct this, including advising of changes to procedures if necessary. The DPO will also identify whether the Information Commissioner's Office (ICO) should be informed. If so, this must occur within 72 hours of discovery of the breach. In making this decision, the DPO must assess the potential negative consequences for individuals of the data breach, namely if there is a risk to people's rights and freedoms.

In the aftermath of a data breach, an investigation should be carried out, led by the DPO or a Trustee as appropriate. Investigation findings will include recommendations for improvements or amendments to existing practises, to avoid a repeat and ensure the Trust is handling data securely. It will be the responsibility of the DPO to oversee the implementation of any such recommendations.



A record of any breach must be filed by the DPO in a Data Breach Log. Any copies of related correspondence and investigative reports should also be filed.

Further guidance regarding data breaches can be found at https://ico.org.uk/fororganisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/.

Information Distribution (internal):

Information should only be shared with members of staff, Trustees or certified volunteers who have a direct interest in the content and where the content is directly relevant to their work.

Internal sharing of information should be done using approved systems only. This means that any files or folders should only be accessible by approved persons, and the information itself should not be distributed outside of those systems.

On occasion it may be required to send information within the organisation by email. This should be done using the minimum information required. On no occasion should information be distributed using BCC function in email.

External distribution (Data Transfers):

Data is only transferred for legal and necessary purposes, utilising a process that ensures such data is transmitted securely and, where possible, is also subject to data minimisation. It is the responsibility of the relevant member of staff/ Designated Safeguarding Lead (DSL) to ascertain whether information should be shared with an external agency, in consultation with the DPO.

Approved, secure methods of transfer must always be used.

Data storage:

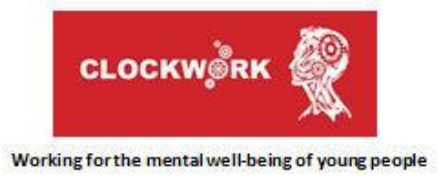
Information is stored on a long-term basis in the following formats:

- Documents on a secure file server.
- All paper-based information will be kept in lockable storage with access available to approved persons only. Paper based information is subject to procedures for storage length, archiving and destruction.

Information may be stored on a short-term basis in the following formats:

- Approved portable PCs or USBs, with multi-factor authentication used to access data. Files stored locally on laptops or USBs must be encrypted e.g. password protected.
- Paper-based for the purposes of assessments and meetings.

When such devices contain this information they must be kept in locked storage when not in direct use, and the information must be deleted once no longer needed.



A separate record summarising the type of information that is stored on these devices should be kept in case of theft.

Records of Data Processing Activities:

The Trust will maintain records of all data processing activities. Internal records will contain the following information:

- The name of who has processed the data; relevant contact details; and the name and contact details of the Data Protection Officer;
- The purposes of the processing;
- A description of the categories of data subjects and of the categories of personal data;
- The categories of recipients to whom the personal data has or will be disclosed;
- Where possible, the envisaged time limits for erasure of the different categories of data;
- A general description of the processing security measures.

Data Retention:

The Information Commissioner obliges the Clockwork Charitable Trust to:

- Adhere to all of the rights of the GDPR;
- Review the length of time personal data is kept (taking into account document retention requirements under UK law). The purpose for holding such information should be considered when deciding whether to retain personal data, and how long for;
- Securely delete information that is no longer needed for the purposes identified ;
- Update, archive or securely delete information if it goes out of date.

All business contracts, agreements and arrangements will be stored for the length of the contract, and for a period of 7 years afterwards.

VAT records will be stored for an indefinite period, and a minimum of 7 years.

Company accounts are kept for an indefinite period, and a minimum of 7 years.

Board meeting minutes, resolutions, and details of company directors are kept for an indefinite period, and a minimum of 7 years.

All financial records may be kept indefinitely, and for a minimum of 7 years.

Personal data of employees in network systems, computer systems and other internal management/administration is not subject to minimum or maximum retention requirements.

All employment contract records, training records, written particulars of employment, identification documents, changes to terms and conditions, working time regulations, correspondence and other agreements between the Trust and an employee are kept for a minimum period of 3 years and a maximum period of 6 years after termination of employment.

Working for the mental well-being of young people

Data of rejected job applicants will be put beyond use or destroyed, unless the applicant wishes to remain on file for future posts.

All individual service user files; daily registration sheets; record of complaints; accident reports and data breach reports will be kept indefinitely, and for a minimum of 3 years.

All data stored externally, on approved and secure systems, will be encrypted and password protected. Security permissions will be set for all electronic data access.

All paper records will be kept in a secure location, with access limited to approved individuals.

The destruction of bulk hardware data must be carried out by a computer company, which erases all remaining information on the hard disk using software approved by CESG, to the Infosec 5 standard.