Thirsk Community Care

CONFIDENTIALITY AND DATA PROTECTION POLICY

Applicable as from May 25 2018

- ## Key Principles

  As set out by The General Data Protection Regulations 2018
  Information held by Thirsk Community Care about living and identifiable individuals whether on computers, data bases or in paper files within the scope of the GDPR comply with the key principles. These are that personal data must be:

- Obtained and processed with fairness, lawfulness and transparency.
- Held only for limited purposes
- Adequate, relevant and not excessive (data minimisation)
- Accurate and up to date
- Not kept longer than necessary (storage limitation)
- Integrity and confidentiality
- Accountability

  These principles are set out in our Privacy Statement

  Thirsk Community Care holds personal information about Trustees, Staff, Clients and Volunteers. We will hold this information whilst you are actively involved with our Charity, or you have given specific consent to keep it or we have a legal requirement to keep it. We will only use this information for the purpose it was given; in order to support clients in line with the purpose of our charity. We will also use it to keep you updated about our current news and events. We will keep personal information accurate and safe and inform you if there is a breach of your personal information. You are to assume that all personal data is held with integrity and confidentiality. You have the right to request what information we hold about you. Please send a written request to The Chief Officer and we will reply within 28 days.

- ## Personal Data

  This includes anything that could directly or indirectly identify someone including:

- Name, contact information
- Family and lifestyle details
- Education and training records
- Medical records
- Employment details
- Financial details

  A name is not essential e.g. if a payroll number is known this could be sufficient.

- **Exceptions**
  Exceptions are personal information shared by data subjects on social networking, information shared through business and commercial activity and household exception.

- ## Special categories of Personal Data

  GDPR prohibits the processing, without good reason, of data that reveals a data subjects:

- Race or ethnicity
- Political opinions, religious or philosophical beliefs
- Trade Union membership

- Genetic Information
- Biometric data
- Health Records

Data Controller

Thirsk Community Care is a Data Controller as we determine the scope and purpose of data to be collected and the means of collection

Data Processor

Thirsk Community Care is a data processor. Thirsk community Care also employs and works with individuals and organisations who process data on behalf of Thirsk Community Care including pay roll and IT support.
The Data processors collect, store, retrieve, organise, file, use, replicate, disseminate and delete personal data.

Requirements for processing Personal Data

In order to process personal data we will satisfy one of the following conditions:

- The clear, explicit and informed consent of the data subject
- The processing is necessary for the performance of a contract with the dat subject or to take steps preparatory for a contract
- Necessary for a legal obligation eg financial, auditory or employment law
- Necessary to protect the subjects interest or those of another person where the subject is not able to give consent

Requirements for processing Special Categories of Personal Data

In order to process special categories we will satisfy one of the following conditions

- Explicit consent
- Necessary for carrying out obligations under employment or social security law
- Necessary to protect interests of subject incapable of giving consent
- Manifestly made public by the data subject
- For exercise or defence of legal claims in court

- Thirsk Community care will also hold personal data if needed under a contractual duty, for example information about users (organisations and individuals) of the Association's services to relevant funders and their auditors. In these circumstances the Association will clearly indicate to the user in advance of providing the service, the nature of the information that will be disclosed and to whom.

Rights of Data Subjects

Data subjects have a right to know:

- Whether or not Thirsk Community Care processes their personal data
- The purposes of the processing
- The recipient of that data
- The period for which data will be stored
- The source of the data
- The existence of automated decision making
- Request notification of incorrect data
- Be forgotten-the erasure of data where the original purpose no longer applies and where there are no additional public interest, public health or legitimate statistical, historical or archival reasons.
- Not be subject to decision making based solely on automated processing of their data without safeguards.
- Data portability-the right to a copy of personal data in a commonly used and machine readable format.

- ## Request for information

- A request for information will be actioned within 28 days, unless the request is unreasonable or unfounded.
- Any such information will be given in either “word” or “excel” format.

- ## Obligations of Data Controllers

- Thirsk Community Care will ensure agreements with Data Processors cover legal obligations
- Appoint the Chief Officer as the Data Protection Officer
- Maintain records of all data processing activities
- Implement Data protection into the design of any new project

- ## Data Security

  Thirsk Community care will implement appropriate technical and organisational measures to ensure security appropriate to the risks and nature of the data.

- Files or computer files containing personal information about are kept in locked filing cabinets or password protected computer files, accessible to relevant staff, relevant line manager and, if appropriate, the Finance Officer.
- If appropriate files will be encrypted. If USBs are used they will be encrypted.
- All personal information kept on personal electronic devices including lap tops, mobile phones and tablets are password protected.
- All personal information kept by staff and volunteers in order to carry out their role are kept securely.
- A Clean desk policy is in place in the office with spot checks
- All visitors will sign in to the office
- All staff are aware of the locking up procedure

- ## Data Breaches

- Thirsk Community Care has procedures in place to detect, report and manage any breaches of data security
- All staff and volunteers will report any breaches to the Designated data protection officer
- The Data protection officer will report the breach to the ICO if the breach could damage rights and freedoms of individuals e.g. damage to reputation, financial loss, unfair discrimination, other significant economic or social loss
- The Individual will be informed if there is a high risk of such damage.

- ## Information held by the Association

- Information held by the Association relates to voluntary and community organisations, other organisations (including those in the public and private sectors) and individuals (including volunteers, employees, trustees, clients, trainers and consultants) which support, assist, provide services and receive services, or fund voluntary and community organisations.
- Some information is kept to enable the Association’s staff to understand the history, activities and views of users (organisations and individuals) in order to deliver the most appropriate and highest quality services.
- The Association also has a role in putting individuals and organisations in touch with other individuals and organisations, and keeps contact details which may be passed on to any enquirer with the data subjects consent.
- Information about age, gender, geographical location, ethnicity and disability of users is kept for the purposes of monitoring our equal opportunities policy and for reporting back to funders.

- # Access to information

- Information is confidential to the Association as an organisation. Thirsk Community Care staff work as a team and as such, liaise and share information about organisations and individuals. They also keep records, monitoring data and mailing lists relating to their work to ensure the most appropriate and highest quality services for users (organisations and individuals).
- The Association's staff will not withhold information from their line manager or the Chief Officer.
- Where information is sensitive, it will be confidential to the Association's staff dealing with the situation, their line manager and the Chief Officer.
- The Association's staff may have sight of their personnel records by giving 28 days notice in writing to the Chief Officer. Access will not be given in respect of information that was clearly provided in confidence to the Association.
- When working on or photocopying confidential information, staff must ensure, as far as is reasonably practical in an open plan office, that it is not seen by people passing. This also applies to information on computer screens. Particular efforts must be made to ensure that confidential information is not seen by people who are not the Association's staff.

- **Personnel records**
- The names and post held within the Association of staff (including employees, students and secondees) is considered to be in the public domain and may be made freely available in any format to anyone.
- The names, nominating organisation and post held within the board of trustees – and people seeking election or nomination as trustees – is considered to be in the public domain and may be freely available in any format to anyone.
- The information provided by trustees and staff as part of the Register of interests is considered to be in the public domain and may be made freely available in any format to anyone.
- The address, telephone number and email address of Trustees shall be made available to all staff and trustees only and only for the purpose of making contact in furtherance of the Association's governance.
- The home and mobile telephone numbers of staff are confidential but shall be made available to all staff for the purpose of making contact in an emergency or urgent work related matter.
- All material in respect of all candidates, other than the successful candidate, gained during the selection of staff is confidential and shall be retained for twelve months after the effective start date of the staff member or volunteer, at which point it shall be destroyed.
- All information required for the purposes of payroll is confidential and made available only to the Treasurer of the Board of Trustees, the Chief Officer and the staff managing the payroll (as designated by the Chief Officer).
- All other information within personnel records is confidential and can only be made available to the Chair of the Board of Trustees, the Chief Officer, or appointed deputies and relevant line manager.

- **Databases of organisations and other contacts**
  Data about individuals/organisations shall only be used by the Association for:

- circulating the Association's publications (which could include advertising), information about the Association and its work, via regular mailings e.g. newsletters, training schedules to all on that particular database.
- To set up rotas for supporting clients
- To enable invoicing of clients
- To provide information to donors and funders
- For any other reason which has been specifically agreed with that individual/ organisation in advance.

- **Specific matters relating to confidentiality.**

- Any correspondence marked private and confidential must be opened by the addressee only. If addressee likely to be absent for more than 2 weeks, then a designated manager will open the correspondence.
- Staff members must ensure that personal papers or records relating to service users, volunteers or any other individual must be kept in a locked cabinet when not being used, or when in use, then out of sight of persons not employed by Thirsk Community Care.
- Confidential interviews must be held in an appropriate location to ensure that any personal information is not overheard.
- Care should be taken to ensure when any records are destroyed, this is done effectively with documents being shredded when appropriate.

- **Breach of Confidentiality**

- Staff who are dissatisfied with the conduct or actions of other staff or the Association should raise this with the Data Protection Officer.
- Staff accessing unauthorised files or breaching confidentially may face disciplinary action. Ex-staff breaching confidentiality may face legal action.
- Data subjects who are dissatisfied with the conduct or actions of staff of the Association should raise this with the Data Protection Officer using the complaints procedure.

- Revised May 2018 and adopted May 25th 2018