Turtle Dove Cambridge Community Interest Company

Data Protection and GDPR Policy

Reviewed: May 2025

Review due: May 2026

Scope of Policy

This policy covers all Subject Data held by Turtle Dove Cambridge (TDC) either in paper or electronic format and the way it is handled. It is subject to the terms of the 2018 General Data Protection Regulations (GDPR).

Introduction

This policy sets out in a clear and concise way to our staff, volunteers, trustees and service users exactly how we will handle data within our organisation.

Information about individuals, whether kept on a computer or in paper format, falls within the scope of GDPR and must comply with the data protection principles. These are that personal data must be:

- Obtained and processed fairly and lawfully
- Held only for specified purposes
- Adequate, relevant and not excessive (in line with the principle of data minimisation)
- Accurate and up to date
- Not kept longer than necessary
- Processed in accordance with GDPR
- Kept secure and protected
- Not transferred outside of Europe

TDC are committed to:

- Holding information in a safe and secure manner and only using the information for the purpose for which it was given.
- Keeping data up to date and accurate.
- Removing out of date data from our records and disposing of it securely.
- Reviewing our policy on a regular basis to ensure that it still meets the needs of the organisation and its members
- Not transferring data outside the EEA.

Data Collection

Why we collect data

We collect information:

- which we are required to report to funders on under grant or Service Level Agreements.
- on our staff and board of directors to enable us to manage our staff policies and payroll.
- on our volunteers to enable us appropriately manage and support them.
- on our service users to enable us to deliver our service.
- on other contacts to help us run our business efficiently.

How we collect data

We collect information from:

- referring agencies and referral forms
- people who contact us
- contacts we make in the course of our activities.

The Data Controller (Managing Director)

The designated Data Controller will deal with the implementation of the agreed policy and day-to-day matters. TDC has a designated Data Controller, the Managing Director, Kate Nation.

Storing and processing data

Our policy is to store all data in a secure manner and to dispose of data no longer required in a secure way. We will process data in a way which is consistent with the aims of our organisation and the purpose for which the data was given. TDC will keep an up-to-date data register. This provides details on personal data processed by the organisation, why it is being processed, the categories of individuals and categories of personal data along with the retention schedules of each type of data (further information can be found under point 5.1 and in Appendix A).

Data in paper form will be kept in filing cabinets that will be kept locked overnight and when not in use. Data in paper format will be shredded before it is disposed of.

Electronic data will be password protected and stored on a server system with regular back up (which will be held off site). Passwords will be reviewed and changed periodically and will always be changed if a member of staff or volunteer with password access leaves the organisation.

Data in either format will only be taken out of the office with the agreement of the Data Controller.

Bring Your Own Device guidance

Typically this relates to smart phones, tablets and USB memory sticks.

- Data stored by TDC should never be transferred to a personal device unless the device is protected by a password (encryption is required if the data relates to information that would identify an individual) and permission for the transfer has been given by TDC's Data Controller and agreement on how long the data may remain on the device is formalised.
- When transferring data from personal devices using a secure channel is critical. Public Wi-Fi networks may not be secure and, therefore, should not be used for this purpose.

- If members of TDC store personal data on a mobile device steps to prevent the data being accessed if the device is lost or stolen must be in place. For example, in addition to encryption, individuals might register the device with a remote locate and wipe facility.
- When someone leaves the organisation TDC will ensure the individual has deleted all information related to TDC.

Retention of data

TDC will keep some forms of information longer than others. TDC will need to keep central personnel records for 6 years after employment ceases. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references. Retention of all other documents and paperwork are detailed on Appendix A.

Under GDPR, the right to be forgotten enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. TDC will give all requests for data deletion or removal thorough consideration and will only retain data following this if there is a compelling reason which will be communicated to the individual concerned.

Processing sensitive information

Sometimes it is necessary to process sensitive information about a person such as race, gender or family details. This is done to ensure that TDC can operate policies on matters such as equal opportunities. TDC may also ask for information about particular health needs or disabilities. TDC will only use such information in the protection of the health and safety of the individual, but will need consent to process - for example, in the event of a medical emergency.

When information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, employees and others affected individuals will be asked to give express consent for TDC to process this data.

Disclosure

It is TDC's policy not to disclose any information to third parties unless TDC has sought the subject's permission to do so OR the information is being passed solely for the third party to undertake work on TDC's behalf and for no other purpose OR the information is already in the public domain OR TDC are legally obliged to do so.

Information will not normally be disclosed. Where information is being passed to a third-party undertaking work on behalf of the organisation TDC will ensure that the third party has appropriate data protection policies and procedures in place.

Confidentiality

TDC recognises that colleagues (employees, volunteers and Directors) gain information about individuals and organisations during the course of their work or activities. In most cases such information will not be stated as confidential and colleagues may have to exercise common sense and discretion in identifying whether information is expected to be confidential.

Information belongs to the person or agency entrusting it to a member of staff or volunteer of TDC. Information remains personal and in the control of the giver. Once received by TDC, it may not be used for any purpose other than that for which it was given; nor may it be passed on to any person or agency outside TDC without the express permission of the giver.

In practice this means that TDC will follow the guidance below:

- Staff members, Directors and volunteers have the right to see any information that TDC keeps on them in paper or computer files and to change that information where it is inaccurate.
- People issues will remain confidential to the people involved.
- TDC will maintain an appropriate level of security, in accordance with the Data Protection Act and the Data Protection Regulations from 25th May 2018 and this policy, which will adequately protect information about individuals that is held in their systems. Paper files will be kept in a locked area and computer-based files will be password protected.
- The use of statistical data or information for reports, monitoring and funding applications will scrupulously avoid any specific detail about service users that might lead to their identification unless they have given their permission for it to be used. The data provided by TDC should not include information that could easily lead to the identification of service users.
- The purpose of information gathered from organisations which is intended to be made public in a Directory, either printed on paper or electronically, must be made clear to those organisations. They must check the accuracy of the information and consent to its distribution obtained before publication.
- Colleagues are able to share information with their line manager in order to discuss issues and seek advice.
- Colleagues will avoid exchanging personal information about individuals with whom they have a professional relationship.
- Colleagues will not disclose to anyone, other than their line manager, any information considered sensitive, personal, financial or private without the knowledge or consent of the individual.
- Where there is a legal duty on TDC to disclose information, the individual will be informed that disclosure has or will be made.

Breaking confidentiality

In exceptional circumstances, it may be necessary to break the basic rules of confidentiality. This would be the case in situations where the safety, rights and liberties of other people or

the person giving information may be seriously at risk. In such cases, staff and volunteers should discuss the matter with their line manager and as appropriate, the Directors. Decisions that are made, and the reasons for them, must be properly recorded.

When confidential information is divulged without consent, except where it might result in more harm to other people, the individual concerned should be informed and an explanation of the action given.

Employees who are dissatisfied with the conduct or actions of other colleagues or TDC should raise the matter with their line manager, using the grievance procedure if necessary, and not discuss it outside TDC.

Breaches of the confidentiality may result in disciplinary action.

Rights of the individual to access information (S.A.R.s)

Employees and other users / members of TDC have the right to access any personal data that is being kept about them either on computer or in other types of files. Should any person wish to exercise this right they should contact the Data Protection Controller.

In order to gain access, a request should be made in writing to the Data Protection Controller.

TDC aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 1 month.

Inaccurate Data

Where an individual advises that their data is inaccurate TDC will ensure the inaccuracy is corrected within 7 working days.

Complaints

Any complaints about the way TDC handles or uses data will be dealt with under the Complaints Policy and Procedure.

Overseas Transfer

It is our policy not to transfer any data overseas.

Conclusion

Compliance with GDPR is the responsibility of all staff, volunteers, trustees and members of TDC. Any deliberate breach of the Data Protection and GDPR Policy may lead to disciplinary action being taken, or access to TDC facilities being withdrawn, or even a criminal prosecution.

Any questions or concerns about the interpretation or operation of this Policy should be taken up with the Data Controller.

Appendix A

Document retention periods relating to staff and accounts

Record	Statutory retention period	Statutory authority and/or Reason for retention
Personnel files including records and notes of disciplinary and grievance hearings	6 years from the end of employment	Potential litigation and references
Application forms/interview notes (unsuccessful applicants)	At least 6 months from the date of the interviews	Time limits on litigation
Facts relating to redundancies where less than 20	6 years from the date of the redundancy	Time limits on litigation
Accident books, accident records/reports	3 years after the date of the last entry (see below for accidents involving chemicals or asbestos)	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (amended April 2012) (SI 1995/3163) as amended
Accounting records	6 years for public limited companies (unless specified otherwise)	Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006
Income tax and NI returns, income tax records and correspondence with HMRC	Not less than 3 years after the end of the financial year to which they relate	The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631)
Retirement Benefits Schemes – records of notifiable events, for example, relating to incapacity	6 years from the end of the scheme year in which the event took place	The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)

Record	Statutory retention period	Statutory authority and/or Reason for retention
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence	3 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) (Amendment 2005) as amended
Statutory Sick Pay records, calculations, certificates, self-certificates	3 years after the End of the tax year to which they relate	The Statutory Sick Pay (General) (Amendment) Regulations 2008
Wage/salary records (also overtime, bonuses, expenses)	6 years	Taxes Management Act 1970
National minimum wage records	3 years after the end of the pay reference period following the one that the records cover	National Minimum Wage (Amendment) Regulations 2011
Records relating to working time	2 years from date on which they were made	The Working Time Regulations 1998 (SI 1998/1833) Working Time Regulations (Amendment) Regulations 2009