Triangle Community Garden

Confidentiality & Data Protection Policy

Revision History

Date	Details	Author	Review Date
June 2013	New policy	L Wills	Feb 2014
Feb 2014	Policy reviewed	L Wills	Feb 2017
May 2018	Policy revised for GDPR	V Wyer	May 2021
Jun 2022	Reviewed	V Wyer	Jun 2025

Introduction

1. The fundamental principles which the Triangle Community Garden (TCG) will observe are:

    - **Integrity, honesty and courtesy** will be the hallmark of all conduct when dealing with colleagues within TCG, volunteers, other individuals and outside organisations;
    - **Accountability** - everything TCG does must be able to withstand the scrutiny of the public, media, funders, and all those connected with the organisation;
    - **Transparency** – TCG will maintain an atmosphere of openness throughout the organisation.

2. The two areas covered by this policy, data protection and confidentiality, relate to the handling and sharing of information.

3. The law that relates to the keeping and sharing of written or electronic information about individuals is set out in the General Data Protection Regulation (GDPR) which comes into force on 25 May 2018 and overrides the provisions of the Data Protection Act 1998 (DPA). Staff and trustees must be aware of their obligations under the GDPR and follow them at all times.

4. Information which is not subject to the GDPR can normally be shared openly and freely. If a trustee or member of staff considers that any information should be kept confidential, then in sharing that information with anyone else they will state clearly that confidentiality is required, the reason why confidentiality is required, and the period of time that confidentiality is required for.

5. Related policies: Whistleblowing, Safeguarding Adults from Abuse, Safeguarding Children, and Creation and Storage of Records (including Sharing).

Responsibility

6. TCG allocates responsibility for compliance to the GDPR to a designated individual who is known as the Data Protection Officer. The Data Protection Officer is should not be involved in day to day data processing.
   The TCG's Data Protection Officer is ……

Definitions:

Data Controller: A data controller determines the purposes and means of processing personal data. TCG acts as a data controller for the data kept by the organisation in pursuance of its charitable objects and to keep its supporters informed of its activities. Controllers are not relieved of their obligations where a data processor is involved – the GDPR places further obligations on controllers to ensure their contracts with processors comply with the GDPR.

Data Processor: A data processor is responsible for processing personal data on behalf of a controller. TCG acts as a data processor with regard to data it collects and stores on its staff, volunteers and service users. For sending out monthly email updates to TCG supporters, TCG uses MailChimp to act as a data processor on its behalf. The GDPR places specific legal obligations on processors; for example, they are required to maintain records of personal data and processing activities. They will have legal liability if you are responsible for a breach

Personal data: any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.
The GDPR definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This includes chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive Personal Data: The GDPR refers to sensitive personal data as "special categories of personal data" (see GDPR Article 9).

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see GDPR Article 10).

Data Protection under the GDPR

7. The operation of TCG requires the collection and storage of certain information on staff, trustees, volunteers, supporters and service users, and of people who are applying to become any of these. TCG will ensure that any personal information is held in compliance with the rights of the individual in accordance with the eight data protection principles set out in the GDPR.

8. **The eight data protection principles require that:**

1) Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless
    a. at least one of the conditions in Schedule 2 is met, and
    b. in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2) Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4) Personal data shall be accurate and, where necessary, kept up to date.

5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6) Personal data shall be processed in accordance with the rights of data subjects under this Act.

7) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8) Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

9. **Schedule 2:** At least one of the following **six conditions** must be met for personal information to be considered fairly processed:

    a. Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
    b. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
    c. Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
    d. Vital interests: the processing is necessary to protect someone's life.
    e. Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
    f. Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Sensitive personal information

10. The GDPR makes specific provision for processing sensitive personal information. This includes racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health condition, sex life, criminal proceedings or convictions.

11. **Schedule 3:** For sensitive personal information to be considered fairly processed, at least one of several extra conditions must be met. These include:

    a. The individual whom the sensitive personal data is about has given explicit consent to the processing.
    b. The processing is necessary so that you can comply with employment law.
    c. The processing is necessary to protect the vital interests of:
        - the individual (in a case where the individual's consent cannot be given or reasonably obtained), or
        - another person (in a case where the individual's consent has been unreasonably withheld).
    d. The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition.
    e. The individual has deliberately made the information public.
    f. The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.
    g. The processing is necessary for administering justice, or for exercising statutory or govern-mental functions.
    h. The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.
    i. The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.

Rights under the GDPR

12. To protect an individual's rights under the GDPR, TCG will ensure that all personal information which it holds is held in accordance with the eight principles. In particular, it will ensure that all such information is held securely and not retained longer than necessary.
13. TCG notes **the right to subject access,** which allows people to find out what information TCG holds about them. The trustees are responsible for responding to any subject access request, and will always respond to such requests promptly and in writing within one month. As a charity the GDPR permits TCG to refuse, or levy a reasonable fee, if the request is unfounded or excessive.

14. TCG notes **the right to be forgotten -** 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. This replaces the 'right to prevent processing', which under the DPA allowed people to ask TCG not to process information relating to him or her that causes substantial unwarranted damage or distress to them or anyone else. The trustees are responsible for responding to any request to be forgotten, and will always respond to such requests promptly and in writing, within one month.

15. **Demonstrating Compliance:** TCG will ensure that it holds an up-to-date register that provides details on all personal data (both ordinary and sensitive) processed by the organisation, and by other organisations on its behalf, why it is being processed, the lawful basis for that processing, the categories of individuals and categories of personal data retained, how that data will be stored, who will have access to it, how long it should be retained.

16. **Avoiding unauthorised access to data** Appendix 1 sets out the steps should staff take to ensure that there is no unauthorised access to the data (for example, drawers must be locked, screens should be locked when staff step away from their desks etc)

17. **Procedure for taking data off site:** Appendix 2 sets out in what form data should be taken off site and how that data should be kept secure (for example that only encrypted data sticks must be used, that any manual files are logged out and back in, that leaving files on car seats is considered a security breach etc)

18. **Breach of security:** Appendix 3 sets out the process that should be followed if there is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Confidentiality

19. Personal information about individuals must always be handled in accordance with the GDPR. The following paragraphs concern information which is not personal information but which may otherwise be confidential.

20. Paid and unpaid staff and trustees of TCG may, from time to time, be in receipt of confidential information as a result of their participation in the normal operation of TCG. How they treat this information may have serious consequences for their own and TCG's reputation and credibility. It may also have employment and legal consequences. To avoid these outcomes the following policy guidelines must be followed.

21. The principle of transparency means that TCG is committed to being open about the information it holds and the way it works. It encourages staff, trustees, volunteers and members of the public to ask questions, and does not fear scrutiny.

22. If there is a need to keep information confidential, then the person sharing that information with anyone else will make clear that there is a need for confidentiality, the reason why, and any time period for which confidentiality is required. Such a request for confidentiality should be respected, unless there is a specific reason that it cannot be.

23. As a matter of courtesy, information relating to the activities of TCG that is not in the public domain, and which is acquired during the ordinary course of work, at board or special meetings, in circumstances where the recipient might reasonably suppose the information to be confidential, should not be disclosed without discussion first with other people who have been party to the conversation.

Ethical obligations

24. These are particularly relevant when dealing with children and adults at risk of abuse. Staff, trustees or volunteers should always disclose information without consent where failure to do so may place a child or adult at risk of death or serious harm or where the information would prevent, detect or prosecute a crime. Refer also to TCG's Safeguarding Policies for Children and Adults at Risk of Abuse.

Publication

- This policy will be available at Ransom's Pavilion, and on the Triangle Garden website: www.trianglegarden.org. It is available on request in hard copy – please email liz@trianglegarden.org or write to Triangle Community Garden, c/o Hitchin Initiative, 1A Churchyard, Hitchin SG5 1HR.
- Current and new members of staff, GA volunteers, service users and trustees will be made aware of its existence and any revisions made.
- Anyone with any concerns about non-compliance with this policy should refer to our Complaints and/or Whistleblowing Policies