

Trefoil Guild Managing information policy

1. Purpose

The Trefoil Guild is an organisation which manages personal data and information every day. We couldn't operate without it. All our staff and members must make sure they collect and use information appropriately, and in line with our Trefoil policies, its code of conduct and the Data Protection Act 2018.

The purpose of this policy is to provide our staff and our members with an overview of how to manage information safely, together with procedures to follow for good practice. It outlines the requirements of the Data Protection Act and how the 7 GDPR principles apply Trefoil Guild data which all must adhere to.

This policy covers:

- [Governance and compliance](#)
- [The Data Protection Act and GDPR](#)
- Our members' rights
- [Information security](#)
- [Data breaches and how to report an incident](#)
- [Records management good practice](#)

2. Scope

This policy is intended to support trustees, staff, and all members within the Trefoil Guild to understand their roles and responsibilities in respect to managing information and the Data Protection Act.

While data protection legislation only applies to personal data, The Trefoil Guild requires its trustees, members, and staff to follow this policy and its supporting procedures when processing any kind of information, personal or otherwise belonging to The Trefoil Guild, to always ensure best practice.

For the avoidance of doubt information management relates to all information whether processed in a paper or electronic format.

3. Governance

3.1 The board of trustees

The board of trustees is accountable for this policy and ensuring that The Trefoil Guild, its staff, and its members comply to the policy and the Data Protection Act.

3.2 Data Protection officer

A Data Protection officer has been appointed by the board of trustees to manage compliance of Data Protection and information management. This role

is undertaken by the manager of the Trefoil Guild office. In the absence of the Data Protection officer due to illness or leave, the role will be covered by the chair of finance and general purposes and the national chair who will also support the officer in their role.

The officer is required to have an understanding of the relevant information governance and data protection legislation and is the point of contact with the Information Commissioners Office (ICO) and for any queries from staff, members and the wider public.

They annually renew The Trefoil Guild registration (Z9153303), as a data controller see appendix definitions with the Information Commissioners Office and advise the Finance and General Purposes Committee when complete.

3.3 Staff and member training

It is a recommendation of The Trefoil Guild that all staff, trustees, and those members with access to KEY the membership database or who hold chair, secretary, treasurer or adviser roles at country, region or county level undertake basic information governance and digital security training.

4. The Data Protection Act 2018 and GDPR

4.1 The legal framework

The Data Protection Act 2018 focusses on **personal data** and we all have a legal duty to comply with the Act.

Personal information is **any** data or information that allows you to identify an individual either on its own or with other factors. It includes things like for example your name, postal address, email address, date of birth, photo, someone's voice, video, or social media handle.

The Act also covers data which is classified as sensitive or special data, and this includes ethnicity, religion, gender identity and health data. You need *explicit* consent to collect this type of data.

4.2 The GDPR principles

The GDPR principles form part of the Data Protection Act and if we should follow these seven simple principles in all we do. The seven principles are:

1. **Fair, transparent, and lawful.** We need to let people know what data we hold about them, how we plan to use it, and if we are going to share it.
2. **Purpose limitation.** Data should only be used for the purpose it was given and not shared without explicit consent.
3. **Adequate, relevant, and limited.** Only the data you need should be collected using the correct and most up to date Trefoil forms from the website.
4. **Accuracy.** Any data you hold **must** be kept up to date. Remember all members have a responsibility to keep their data correct either directly onto the website or by contacting the membership helpline
5. **Time limited.** Only keep data for as long as it is needed. You can check how long you can keep data in the Trefoil "Data Retention Policy"
6. **Keep data** with integrity and confidentiality. Keep data secure whether on paper or held digitally/electronic.
7. **Accountability.** We are all responsible for the data we hold and access and for adhering to Trefoil policies and procedures, the Data Protection Act and GDPR and for following the Trefoil code of conduct.

These principles apply to all levels within Trefoil and if you keep any local records, you may breach the Data Protection Act if you do not apply the GDPR principles.

4.3 Data sharing

The main reason why we collect information in Trefoil is for '**legitimate interest**'. Trefoil makes it clear in our **Privacy policy** what personal data we collect and who we share it with.

Data can only be shared outside our Privacy policy with **explicit** consent. That means asking all members concerned and being able to demonstrate that they have been asked.

On those occasions when we do need to share information only share the minimum amount needed, e.g., those manning registration at an event only need the name of the member attending, not their home address and telephone number.

Sharing personal information is also allowed if it's in the **vital interest** of a member, perhaps in the event of a medical emergency. In addition, when it is in the public interest or when there is a legal basis for sharing, for safety or for safeguarding sharing is allowed but this can be a complex area, so for this and all approaches from police or legal teams contact the Trefoil office.

5. Our members' rights

Data protection and GDPR is regulated by the Information Commissioners Office (ICO) whose role is to uphold information rights in the public interest. This means that our staff and members have legal rights in respect to any data we hold, whether that is at a national, country or region, county or local Trefoil Guild level. These rights can be summarised as:

- **A right to be informed** about the collection and use of their personal data
- **A right of access**, that is to receive a copy of any of their personal data held
- **A right to update it**, so that any inaccurate or incomplete information can be updated. **All members can update or correct their own information via their members account on the website or by phoning the helpline on 0151 6680493**
- **A right to move it (portability), to delete it or limit it.** Whilst members do have a right to have personal data erased or request limiting processing of their personal data this may not be possible for legal reasons or may make being a member impossible.

If you would like to progress any of these rights, please contact the Trefoil Guild office manager via email to trefoilguild@girlguiding.org.uk or in writing to The Trefoil Guild, 17-19 Buckingham Palace Road, London, SW1W 0PT, including your name and membership number with your request. We will aim to respond within ten working days from receipt of your request.

6. Information security

As staff, trustees, or members of The Trefoil Guild, if you hold or process information on behalf of The Trefoil Guild you are responsible for making sure that data security is always maintained irrespective of whether that information is in paper or electronic form. You should take all necessary precautions to protect our own and members data including but not limited to:

- Having good system and device security
- Ensuring any personal data held, or circulated electronically is secured with a *strong* password
- Using safe and secure processes when sending, receiving or storing digital and hard copy communications and documents
- By adhering to the **Trefoil Policies and the Trefoil code of conduct**
- By following the **Data Protection legislation and seven GDPR principles.**

The Trefoil Guild will take appropriate steps to ensure that appropriate technical and organisational measures are taken to prevent unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

6.1 Secure access to our membership system

To enhance the security of Trefoil's data, all staff and members who use KEY, our membership database, are required to use 'multifactor authentication' (MFA). This has enhanced security over simple usernames and passwords and gives increased confidence against cyber criminals. Likewise, 'two factor authentication' (2FA) has been enabled for member accounts on the website.

7. Data breaches

By a 'data breach', we mean where personal data or devices holding personal data, has been lost, stolen, accessed or shared inappropriately.

By following this Managing Information policy and attending training courses as relevant to your role, the chances of a data breach are minimised.

There are many examples of data breaches which include things like a stolen or lost device, not using blind carbon copy (bcc) in group emails, attaching unprotected documents containing personal data in an email, having directories circulated without passwords or leaving paper copies of directories at venues or on public transport.

7.1 Data breach procedure

There are four stages to the Trefoil data breach procedure:

A. Reporting a data breach: report your data breach within 24 hours using the 'data breach notification form' in appendix B (also available as a separate form on the website for ease of use) or contact the Trefoil office on 0207 834 6242 Extension: 3010.

You must report the breach even if you managed to retrieve any lost information or stolen device. By law, Trefoil need to maintain a record of all actual and potential breaches.

Depending on the nature and severity of the data breach and following assessment The Trefoil Guild may be required to notify the Information Commissioners Office (ICO) which is the UK regulatory body.

Where the breach poses a high risk to the rights and freedom of the individual(s) involved in the breach, they would also be informed as would any 3rd parties who could assist in mitigating the impact of the breach such as IT suppliers, police, insurers, professional bodies, banks and credit card companies.

B. Containment and recovery: By quickly acting many data breaches can be contained reducing or minimising the impact. These include such things as

- recalling an email
- contacting the recipient (s) of an email and ask for them to delete it from their account and their email 'bin' folder.
- If devices or documents have been lost attempt to find them or if stolen report the loss
- contacting the Trefoil office for advice on 0207 834 6242 Extension: 3010

C. Assessment and evaluation of the breach: The Trefoil Data Protection officer will assess the severity of the breach using a series of questions based on the Information Commissioners guidance or by using the online tool [Self-assessment for data breaches ICO](#). This indicator is then used as a recommendation to the chair of finance and general purposes or the national chair in reporting to the ICO.

All breaches are recorded on a log at the Trefoil Guild office which is circulated and discussed at all finance and general purposes committee meetings to ensure that necessary actions are identified and undertaken.

All breaches are then evaluated to understand the circumstances of the breach and understand the root cause.

D. Review and response: After a breach there may be a number of actions that are required to be taken by the individual (s) who contributed to the breach occurring, such as putting in additional security measures on their devices or attending training. Some actions may be at organisational level to address lessons learned which could necessitate changes to policy, processes or procedures to prevent future occurrences in the future.

8. Records management

All Trefoil records should be managed along the lines of the 7 GDPR principles which simply means that:

- **Records should be current and up to date**
- **Always kept accurate**
- **Be relevant and appropriate**
- **Only kept as long as needed**
- **Kept securely**
- **Only shared with explicit consent or in line with the Trefoil Privacy policy.**

8.1 Collecting or updating data: Remember that once collected, it is your responsibility to ensure that data is accurate, kept up to date and destroyed or deleted when no longer required. Always use the latest Trefoil forms available on the website for data collection if available.

8.2 When and how to get rid of data: Making sure that personal data is destroyed safely and in line with the Data Retention policy. Do not keep personal data for longer than is necessary for the purposes it was collected for. Methods to be used are:

- **For paper or hard copy data:** shred or rip into small pieces so that personal data cannot be read
- **For electronic or digital data:** delete from emails and devices/computer folders. Remembering to also delete from download folders, trash bins and cloud storage.

9. Monitoring and compliance

This policy has been approved by the Board of Trustees and the implementation and monitoring of the policy will be undertaken by the finance and general purposes committee.

© The Trefoil Guild
finance and general purposes
17-19 Buckingham Palace Road London
SW1W 0PT

Author: chair of

Version: 2.0
Date: December 2024
Review Date: Dec 2027

Appendix A: Definitions

| term | definition | further information or example |
|------------------|---|--|
| ICO | Information Commissioners Office | UK regulatory body |
| Data controller | A person or an organisation who alone, or with others, decides how and why collected data will be used. | The Trefoil Guild is the data controller for its members personal data and charity records. |
| Data breach | An act or occurrence which causes the loss, destruction and or erasure, alteration, unauthorised disclosure and or sharing of unauthorised access to, unauthorised use and or publication of personal data. | Examples such as emailing personal data to the wrong person or leaving personal data unsupervised or in a public place where others can access it. |
| Data subject | A data subject is a living individual who is the subject of the personal data. | Examples include a Trefoil Guild trustee, employee or member |
| Personal data | Any information relating to an identifiable person or 'data subject'. | Examples include, name, address, telephone number, email address, social media handle, photograph, disability or health data, religion, ethnicity |
| Data processing | The use, collection, storage, and disposal of personal data. | Storing of staff and member data. Sharing member information by email. Shredding when information is no longer required. |
| GDPR | General data protection regulation. | Forms part of the UK Data Protection Act 2018 enforceable by law. |
| Joint Controller | Where two or more (data) controllers jointly determine the purposes and means of processing. | Companies supporting The Trefoil Guild membership system, printing the magazine and providing a help line. |

Appendix B:

Also available on the website as a separate Microsoft Word document

Reporting a data breach and notification form

All Trefoil staff and Trefoil members are responsible for reporting any breach of personal data. That is any situation which leads to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Personal information is **any** data or information that allows you to identify an individual either on its own or with other factors. It includes things like for example your name, postal address, email address, date of birth, photo, someone's voice, video, or social media handle.

Examples of data breaches include but are not limited to things like a stolen or lost devices, not using blind carbon copy (bcc) in group emails, attaching unprotected documents containing personal data in an email, having directories circulated without passwords or leaving paper copies of directories at venues or on public transport.

On discovering a data breach this form **MUST** be completed immediately.

On completion the form to be emailed for the attention of the Trefoil Guild Data Protection officer to trefoilguild@girlguiding.org.uk

If you have problems printing or emailing the form, then please phone the Trefoil Guild office on 020 7834 6242 Ext 3010

Do not worry about reporting the data breach, the Trefoil office staff will help and support you in the management of the incident and once resolved will work with you to prevent reoccurrences.

| Data breach notification form | |
|--|-----------------|
| Trefoil membership number OR if not a member, provide your contact details and describe your relationship to the organisation | Number: T _____ |
| Actual date of the incident | _____ |
| The date when it was discovered? | _____ |
| Briefly describe the incident | |
| What personal data has been placed at risk? | |
| How many people have been affected by the incident? | |
| Has there been any media coverage of the incident? If so, what? | |
| What action has been taken to minimise or mitigate the effect on those involved? | |
| Have you taken any steps to prevent similar incidents in the future? | |

| | |
|---|--|
| | |
| Is there any other information which would assist Trefoil's assessment of the incident? | |