Talking Maths in Public

Data Protection Policy

Key definitions

Personal data: means any information relating to a natural person who can be directly or indirectly identified in particular by reference to an identifier.

Sensitive data: special categories of personal data. These include racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health or sex life, sexual orientation.

Data controller: a natural or legal person (organisation) that collects and processes personal data. The controller is responsible for, and must be able to demonstrate, compliance with the principles of GDPR.

Data Processing: any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1. **Introduction**

1.1. Talking Maths in Public (TMiP) is a Data Controller under the Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulation (GDPR), together referred to in this policy as 'the data protection legislation'. We are a not-for-profit organisation which only processes data for the purposes of running TMiP activities, and are therefore exempt from registering with the Information Commissioner's Office (ICO). In this policy references to "TMiP" or "we" are to the Talking Maths in Public trust.

1.2. TMiP processes personal information of its trustees, contractors, volunteers, partners, event attendees, mailing list members, beneficiaries and other individuals (such as key business contacts). Personal information is kept in a range of forms, including the following:

a) Digital records
b) Paper records
c) Video footage
d) Audio recordings
e) Photographic material

1.3. Such information must be collected and processed in line with the six principles of the data protection legislation. Article 5 of the GDPR states that personal data must be:

1.3.1. Processed lawfully, fairly and in a transparent manner in relation to individuals;

1.3.2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

1.3.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

1.3.4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified;

1.3.5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for long periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

1.3.6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

1.4. TMiP as a Data Controller is responsible for and must be able to demonstrate compliance with these principles.

2. Purpose

2.1. The purpose of this policy is to assist TMiP in meeting its legal obligations under the data protection legislation. It describes the responsibilities of everyone working or volunteering for TMiP, whether trustee, contractor, or volunteer, and the rights of access by individuals to their personal data. This policy is intended to ensure that personal information is handled correctly and securely and in accordance with the data protection legislation.

2.2. Whilst the TMiP board of trustees is ultimately responsible for compliance, and any penalties or undertakings will be addressed to them in the event of a breach, every contractor and volunteer who has access to and/or is responsible for processing data should also be aware of their role in adhering to the policies and procedures of TMiP.

3. Statement of Responsibility

3.1. TMiP, as a data controller with responsibilities under the data protection legislation, will ensure that all handling of personal data complies with the six principles of the data protection legislation by adopting and enforcing policies and procedures that will minimise the risk that personal data will be misused.

3.2. In particular TMiP will ensure that:

3.2.1. Appropriate structures are in place to ensure that there is a chain of responsibility for Data Protection within the organisation;

3.2.2. Data subjects (trustees, partners, contractors, volunteers, event attendees, mailing list subscribers, beneficiaries and contacts) are informed that TMiP collects certain data for specific purposes and on pre-defined lawful bases, through data processing statements (privacy notices and privacy policy);

3.2.3. Data processing notices must be clear and easy to understand, explain the purposes for which and the lawful bases on which the personal data will be processed;

3.2.4. Transparency is maintained in how the information is collected and how it will be used;

3.2.5. Only necessary data is processed and that it is only used for the purposes of the original collection;

3.2.6. Data will not be retained once it is no longer required for its stated purpose (data may be retained for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, as is covered under GDPR legislation);

3.2.7. Data is not processed in a way that would have unjustified adverse effects on the data subject, or for unlawful purposes;

3.2.8. All trustees, contractors and volunteers that have access to or process personal data understand that they are required to abide by this Policy, and the data protection legislation;

3.2.9. Trustees, contractors and volunteers receive the necessary information to be able to adhere to the requirements of the data protection legislation and to prevent as far as possible unintentional data breaches;

3.2.10. Appropriate measures are in place to limit personal data breaches. If a breach does occur, in line with the legislation, TMiP will report the breach to the relevant supervisory authority within the 72 hour guidelines. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, TMiP will inform those individuals without undue delay. In line with GDPR TMiP will keep a record of any personal data breaches, regardless of whether we are required to notify or not.

3.3. The TMiP WhatsApp group was set up by the TMiP board of trustees, but TMiP does not process any data of those members who choose to join; all data on the WhatsApp group is processed by WhatsApp.

4. Data processing procedures

4.1. Data will be processed securely by members of the board of trustees (also known as the TMiP committee) and by any external contractors or volunteers who need access to the data in order to carry out their work for TMiP. Electronic data will only be stored on devices which are not able to be accessed by unauthorised parties or in password-protected cloud storage. Where data is transferred electronically it will be password protected. Hard-copy data will be stored securely.

4.2. Non-anonymised personal data will only be shared outside of the TMiP board of trustees where this is necessary for TMiP activities to run effectively, for example with volunteers registering participants at an event or speakers who need to know accessibility requirements.

5. Subject Access Requests

5.1. Requests received from individuals for a copy of the information TMiP holds on them will be passed to the TMiP Data Protection Officer for processing and may be delegated to another trustee. Requests for personal information need to be made in writing with sufficient supporting evidence to validate the individual's identity to TMiP's satisfaction, and to be able to identify what information is being requested. Requests will be responded to within one month of the date all the information required to be able to fulfil the request is received.

6. Data Protection Officer

6.1. The TMiP board of trustees are jointly responsible for enforcing the measures laid out in this policy.

6.2. The TMiP Data Protection Officer has particular responsibility for processing subject access requests and reporting any data breaches on behalf of the TMiP trust; they may delegate these responsibilities to another TMiP trustee at any time.

6.3. The TMiP Data Protection Officer (DPO) is: Katie Steckles

6.4. You can contact the DPO and the TMiP Board of Trustees by emailing info@talkingmathsinpublic.uk

7. Review

7.1. This Policy will be reviewed by the TMiP Board of Trustees and approved by a board vote every three years, or sooner if regulatory changes require the Policy to be updated.

7.2. Annual reviews of (a) data handling practices within TMiP and (b) the effectiveness of data processing procedures will be undertaken by the TMiP board of trustees to ensure compliance with this Policy.

Adopted by the TMiP Board of Trustees on: 07/04/2019

Last reviewed: 25 Jun 2025