TOYNBEE HALL

DATA PROTECTION POLICY

TOYNBEE HALL

V3.0

Version Control

Amendments

Version	Author	Date	Comments
1.0	D Brady	November 2015	
1.1	D Brady	February 2017	
1.2	D Brady	February 2018	
2.0	Head of Monitoring and Evaluation	August 2021	
3.0	Head of Data & Impact	August 2024	Review of suite of policies by Bulletproof, DPO

Reviewed By

Name	Date	Next Review	Comments
Dan Bunn	August 2021	August 2022	No changes
Dan Bunn	August 2022	August 2023	No changes
Ben Campion	October 2023	November 2023	Minor amends

CONTENTS

1. PURPOSE

The purpose of this policy is to set out Toynbee Hall's approach to data protection and data privacy.

2. INTRODUCTION

The personal data that Toynbee Hall processes to provide advice services, community activities, research and policy, and venue hire to those in receipt of our services and other individuals as necessary, including staff and suppliers' staff. This can include job applicants, temporary and agency workers, contractors, interns, volunteers, and apprentices as well as donors and trustees.

Toynbee Hall processes the personal data of staff/customers/suppliers and others where necessary and is committed to ensuring that all the personal data that it processes is carried out in accordance with all data protection law.

Toynbee Hall ensures that good data protection practice is embedded in the culture of our staff and our organisation.

Toynbee Hall's full suite of data protection policies and procedures are:

-
- Privacy notices (website, clients, employees)
- Data breach Policy
- Data Protection Policy
- IT security policies (data security policy & IT systems use policy)

'Data Protection Law' includes the General Data Protection Regulation 2016/679; the UK Data Protection Act 2018 and all relevant UK data protection legislation.

3. SCOPE

This policy applies to all personal data processed by Toynbee Hall and is part of Toynbee Hall's 's approach to compliance with data protection law. All Toynbee Hall staff, trustees, partners or third parties who have, or may have access to personal data are expected to have read, understood and comply with this policy and failure to comply may lead to disciplinary action for misconduct, including dismissal or contract termination.

4. RESPONSIBILITIES

Toynbee Hall is a data controller and a data processor under the UK GDPR/DPA 2018.

Key responsibilities are:

- All managers are responsible for ensuring personal data is handled in accordance with Toynbee Hall's 's policies and procedures and for encouraging best practice in the handling of personal data.
- The Chief Executive Officer is accountable to the Board of Trustees and for ensuring compliance with data protection law can be demonstrated.
- Compliance with data protection law is the responsibility of all employees, partners and third parties working on behalf of Toynbee Hall
- The CEO is ultimately accountable for ensuring Toynbee Hall is compliant with data protection law

Toynbee Hall will ensure that all staff, partners or third parties who handle personal data on its behalf are aware of their responsibilities under this policy and other relevant data protection and information security policies, and that they are adequately trained and supervised.

Toynbee Hall operates an open reporting policy concerning personal data breaches. People will sometimes make mistakes, but it is only by encouraging open reporting when mistakes occur that lessons are learnt, thereby benefiting the organisation.

Staff should be reassured that they will not be penalised for reporting honest mistakes concerning personal data breaches.

5. DATA PROTECTION PRINCIPLES

Toynbee Hall complies with the data protection principles set out below. When processing personal data, it ensures that:

- It is processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').
- It is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation').
- It is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

- It is accurate and, where necessary, kept up to date and that reasonable steps will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').
- It is 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 ('storage limitation').
- It is 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 ('integrity and confidentiality').

Toynbee Hall is responsible for complying with the data protection principles and will demonstrate this in accordance with Article 5(2) "Accountability" by implementing policies and procedures, technical and organisational measures and keeping documentation such as breach records and Data Subject Rights Request records.

6. DATA SUBJECT RIGHTS

Toynbee Hall has processes in place to ensure that it can facilitate any request made by an individual to exercise their rights under data protection law. All staff have received training and are aware of the rights of data subjects. Staff can identify such a request and know who to send it to.

All requests will be considered without undue delay and satisfied within one calendar month of receipt as far as possible.

Toynbee Hall will ensure the rights as detailed below can be exercised by data subjects.

Informed: The right to be informed about the collection and use of personal data is addressed via company privacy notices.

Subject access: The right to request information about how personal data is being processed, including whether personal data is being processed and the right to be allowed access to that data and to be provided with a copy of that data along with the right to obtain the following information:

- The purpose of the processing.
- The categories of personal data.
- The recipients to whom data have been disclosed or which will be disclosed.
- The retention period.

- Their rights to request rectification, erasure or restriction or to object to processing.
- The right to lodge a complaint with the Information Commissioner's Office.
- The source of the information if not collected direct from the subject; and
- The existence of any automated decision-making (including profiling) and information about the logic involved, significance and envisaged consequences.
- The safeguards provided where personal data has or will be transferred to a third country or international organisation.

Rectification: The right to allow a data subject to rectify inaccurate personal data concerning them or completed if it is incomplete.

Erasure: The right to have data erased and to have confirmation of erasure, but only where (this list is not exhaustive):

- The data is no longer necessary in relation to the purpose for which it was collected, or
- Where consent is withdrawn, or
- Where there is no legal basis for the processing, or
- There is a legal obligation to delete data.

Restriction of processing: the right to ask for certain processing to be restricted in the following circumstances:

- If the accuracy of the personal data is being contested, or
- If our processing is unlawful but the data subject does not want it erased, or
- If the data is no longer needed for the purpose of the processing but it is required by the data subject for the establishment, exercise or defence of legal claims, or
- If the data subject has objected to the processing, and you are considering whether your legitimate grounds override those of the individual

Data portability: the right to receive a copy of personal data which has been provided by the data subject in a structured, commonly used and machine reasonable format. It also allows data subjects to request that a controller transmits this data directly to another controller. This right only applies when the lawful basis is consent or the performance of a contract, and when the processing is being carried out by automated means.

Object to processing: The right to object to the processing of personal data relying on the legitimate interests processing condition unless Toynbee Hall can demonstrate compelling legitimate grounds for the processing which override the interests of the data subject or for the establishment, exercise or defence of legal claims.

Object to automated profiling: The right to object where solely automated decision-making (including profiling) is being carried out that has legal or similarly significant effects on the data subject.

7. SPECIAL CATEGORY DATA

This includes the following personal data revealing:

- Racial or ethnic origin

8. POLITICAL OPINIONS

- Religious or philosophical beliefs
- Trade union membership
- The processing of genetic data, biometric data for the purpose of uniquely identifying a natural person
- An individual's health
- A natural person's sex life or sexual orientation

Criminal convictions and offences is not categorised as special category data, however where processed, will be in line with legislation.

Toynbee Hall will apply additional organisational and technical measures to protect special category data where processed based on risk to the data subject.

Toynbee Hall will only process special category data where it has an Article 6 lawful basis and an Article 9 exception to do so.

9. CONSENT

Toynbee Hall understands the conditions of consent as defined in Article 7 of the GDPR and will ensure that:

- Consent is a specific, informed and unambiguous indication of the data subjects wishes
- The data subject can withdraw consent at any time
- Withdrawal of consent is as easy as it was to give
- Records of consent are kept as evidence

- The data subject is competent to give consent and is doing so freely without duress

This will be ensured through staff training and technical measures implemented to facilitate the above approach.

10. SECURITY

Toynbee Hall will always assess the risk of processing personal data to the data subject and

- Ensure that personal data is stored securely using software that is kept-up-to-date and supported.
- Access to personal data shall be role based, limited to personnel who need access and appropriate security shall be in place to avoid unauthorised sharing of information.
- When personal data is deleted, this shall be done safely such that the data is irrecoverable, where appropriate.
- Appropriate back-up and disaster recovery solutions shall be in place.
- Staff are given information security training and information security policies and procedures are adhered to
- Personal data is encrypted where possible at rest and in transit
- Where possible personal data is anonymised or pseudonymised
- All passwords used meet password policy requirements
- Anti-malware software is deployed on all devices handling personal data
- Paper documents containing personal data shall be stored in lockable cabinets

11. DATA BREACHES

We have a separate Data Breach Policy which can be found at Operational Policies (Health & Safety, Complaints, GDPR, IT). Please ensure you familiarise yourself with this and the Data Breach Procedure to ensure appropriate steps are adhered to and carried out should a personal data breach occur. All personal data breaches must be reported in line with the Data Breach Procedure.

12. DATA TRANSFERS

Toynbee Hall will ensure that any personal data transferred to third countries or third parties in third countries will not be transferred without suitable safeguards which may include:

- UK Addendum with Standard contractual clauses
- International Data Transfer Agreement
- Binding corporate rules
- Adequacy decision
- An exception as defined in Article 49 of the GDPR

Toynbee Hall manages a range of projects. In some cases, the funder my apply additional stipulations regarding data transfers. It is important, that grant agreements and contracts are consulted when making decisions on data transfers.

13. DATA PROTECTION BY DESIGN

Data Protection by Design allows for Data Protection to be built into a business's ethos but ensuring processes, services and other ideas are risk assessed from a GDPR point of view. Toynbee Hall is committed to practicing this throughout the business to ensure systems are built with data protection as the first thought, rather than an afterthought. All staff must declare new processes involving data to ensure this assessment is completed where needed.

14. DATA RETENTION

Data retention schedule in the records of processing activities shall be implemented to ensure that all information kept for legal, regulatory and business requirements is limited. Toynbee Hall will ensure that processes are in place for secure disposal when data no longer needs to be retained for legal, regulatory and business requirements. An automatic or manual executed process is to be in place for identifying and ensuring secure removal of data.

For more information, please view our Data Retention Policy.

15. MONITORING AND REVIEW

This policy shall be regularly monitored and reviewed, on an annual basis or where legislation requires.

The policy is owned by the CEO and compliance, incidents and breaches are overseen by the Audit and Risk Committee.