TOYNBEE HALL

DATA PROTECTION AND GDPR POLICY

TOYNBEE HALL

VERSION 2.0

Toynbee Hall, 28 Commercial Street, London E1 6LS.
Registered Charity No. 211850 Registered No. 20080 England
info@toynbeehall.org.uk www.toynbeehall.org.uk

Contents

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	

Reviewed By

Name	Date	Next Review	Comments
Dan Bunn	August 2021	August 2022	No changes
Dan Bunn	August 2022	August 2023	

Introduction

Toynbee Hall obtains, keeps, and uses personal information (also referred to as data) about clients, job applicants and current and former employees, temporary and agency workers, contractors, interns, volunteers and apprentices as well as donors and trustees for several specific lawful purposes.

This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to our workforce and clients. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal information relating to our workforce and clients, and how (and when) we delete that information once it is no longer required.

Dan Bunn is responsible for informing and advising Toynbee Hall and its staff on its data protection obligations, and for monitoring compliance with those obligations and with Toynbee Hall's policies.

Holly Budgett is responsible for IT/ cybersecurity and insurance and ransomware, phishing or spoof email attacks, use of internet, email and Toynbee Hall provided ICT equipment.

If you have any questions or comments about the content of this policy or if you need further information, you should contact the data protection officer by emailing dpo@toynbeehall.org.uk or by letter to: Toynbee Hall, 28 Commercial Street, London E1 6LS.

By Telephone: +44 (0) 20 7247 6943.

Scope

This policy applies to the trustees, employees (full time, part-time or casual), volunteers and subcontractors of Toynbee Hall, who will be referred to as 'staff' or 'staff members'.

This document is also applicable to our client's other stakeholders in Toynbee Hall.

Toynbee Hall policy and procedure documents may be distributed to suppliers, accreditation and compliance bodies and any other relevant third parties.

In some cases, third parties such as suppliers or those performing on-site work for Toynbee Hall will be expected to adhere to our policies, which will be made available where applicable.

We will review and update this policy following our data protection obligations. It does not form part of any employee's contract of employment, and we may amend, update or supplement it from time to time.

We will circulate any new or modified policy to staff and any other stakeholders when it is adopted.

People and Clients Definition

People/The people we exist to support are also referred to as 'clients' in this document for ease of reading.

People/Clients are community members that Toynbee Hall works with including but not limited to:

- People in housing need
- People in insecure and low paid work
- People dependant on the social safety net of benefits

Definitions

Criminal Records Information	Means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;
Data Breach	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;
Data Subject	Means the individual to whom the personal information relates;
Personal Information	(Sometimes known as personal data) means information relating to an individual who can be

	identified (directly or indirectly) from that information;
Processing Information	Means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;
Pseudonymised	Means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;
Sensitive Personal Information	Sometimes known as 'special categories of personal data' or 'sensitive personal data' means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation and other protected characteristics outlined in the Equality Act
Controller	Art.2(d) GDPR "Controller" means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU or Member State laws, the controller may be designated by those laws.

Data Protection Principles – Clients, Staff, Donors and Trustees

Toynbee Hall will comply with the following data protection principles when processing personal information:

- We will process personal information lawfully, fairly and in a transparent manner;
- We will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;
- We will only process the personal information that is adequate, relevant and necessary for the relevant purposes;
- We will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;
- We will keep personal information for no longer than is necessary for the purposes for which the information is processed; and
- We will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The Basis for Processing Personal Information – Clients, Staff, Donors and Trustees

Concerning any processing activity we will, before the processing starts for the first time, and then regularly while it continues:

- Review the purposes of the processing activity, and select the most appropriate lawful basis (or bases) for that processing, for example:
    - That the data subject has consented to the processing;
    - That the processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject before entering into a contract;
    - That the processing is necessary for compliance with a legal obligation to which Toynbee Hall is subject;
    - That the processing is necessary for the protection of the vital interests of the data subject or another natural person; or

    - That the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or
        - That the processing is necessary for legitimate interests of Toynbee Hall or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.

    - Except where the processing is based on consent, satisfy ourselves that the processing is necessary for the relevant lawful basis (for example, that there is no other reasonable way to achieve that purpose);
    - Document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles.
    - Include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s).
    - Where sensitive personal information is processed, also identify a lawful special condition for processing that information, and document it; and
    - Where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

- Determine whether Toynbee Hall's legitimate interests are the most appropriate basis for lawful processing, we will:

    - Conduct a legitimate interest's assessment (LIA) and keep a record of it, to ensure that we can justify our decision;

    - If the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);

    - Keep the LIA under review, and repeat it if circumstances change; and

    - Include information about our legitimate interests in our relevant privacy notice(s).

Sensitive Personal Information – Clients, Staff, Donors and Trustees

Sensitive personal information is sometimes referred to as 'special categories of personal data' or 'sensitive personal data'.

- Toynbee Hall may need to process sensitive personal information. We will only process sensitive personal information if:
    - We have a lawful basis for doing to set out above, for example, it is necessary for the performance of the employment contract, to comply with Toynbee Hall's legal obligations for people or for Toynbee Hall's legitimate interests; and
    - One of the special conditions for processing sensitive personal information applies, for example:
        - The data subject has given explicit consent so Toynbee Hall can provide its services.
        - The processing is necessary for exercising the employment law rights or obligations of Toynbee Hall or the data subject.
        - The processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent.
        - Processing relates to personal data which are manifestly made public by the data subject.
        - The processing is necessary for the establishment, exercise or defence of legal claims; or
        - The processing is necessary for reasons of substantial public interest.
- Before processing any sensitive personal information, staff must inform the DPO of the proposed processing, so that the data protection officer may assess whether the processing complies with the criteria noted above.
- Sensitive personal information will not be processed until:
    - The assessment/training has been agreed to; and
    - The individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

- Toynbee Hall will not carry out automated decision-making (including profiling) based on an individual's sensitive personal information.

- Toynbee Hall's Privacy Notice sets out the types of sensitive personal information that Toynbee Hall processes, what it is used for and the lawful basis for the processing.

- Concerning sensitive personal information, Toynbee Hall will comply with the procedures set out to make sure that it complies with the data protection principles set out above.

- During the recruitment process: the company will ensure that (except where the law permits otherwise):

    - During the short-listing, interview and decision-making stages, no questions are asked relating to sensitive personal information, for example, race or ethnic origin, trade union membership or health;

    - If sensitive personal information is received, for example, the applicant provides it without being asked for it within their CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted;

    - Any completed equal opportunities monitoring form is kept separate from the individual's application form, and not be seen by the person shortlisting, interviewing or making the recruitment decision;

    - 'Right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages;

    - We will not ask health questions in connection with recruitment.

- During employment: the company will process:

    - Health information to administer sick pay, keeping sickness absence records, monitoring staff attendance and facilitating employment-related health and sickness benefits;

    - Sensitive personal information for equal opportunities monitoring and pay equality reporting. Where possible, this information will be anonymised; and

- Trade union membership information for staff administration and administering 'check off'.

Criminal Records Information - Staff

Criminal records information will be processed following the Toynbee Hall DBS Policy.

Data Protection Impact Assessments (DPIAs) – Clients and Staff

Where the processing is likely to result in a high risk to an individual's data protection rights we will, before commencing the processing, carry out a DPIA to assess:

- Whether the processing is necessary and proportionate concerning its purpose.
- The risks to individuals; and
- What measures can be put in place to address those risks and protect personal information.
- Before any new form of technology is introduced, the manager responsible should therefore contact the data protection officer so that a DPIA can be carried out.
- During any DPIA, the employer will seek the advice of the data protection officer and any other relevant stakeholders.

Documentation and Records - Staff and Trustees

We will keep records of processing activities, including:

- The name and details of the employer's organisation (and where applicable, of other controllers, the employer's representative and DPO);
- The purposes of the processing;
- A description of the categories of individuals and categories of personal data;
- Categories of recipients of personal data;
- Where relevant, details of transfers to third countries, including documentation of the transfer mechanism safeguards in place;
- Where possible, retention schedules; and
- Where possible, a description of technical and organisational security measures.

As part of our record of processing activities we document, or link to documentation, on:

- Information required for privacy notices.
- Records of consent.
- Controller-processor contracts.
- The location of personal information.
- DPIAs; and
- Records of data breaches.

If we process sensitive personal information or criminal records information, we will keep written records of:

- The relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;
- The lawful basis for our processing; and
- Whether we retain and erase the personal information following our policy document and, if not, the reasons for not following our policy.

- We will conduct regular reviews of the personal information we process and update our documentation accordingly. This may include:
    - Carrying out information audits to find out what personal information Toynbee Hall holds.
    - Distributing questionnaires and talking to staff across Toynbee Hall to get a more complete picture of our processing activities; and
    - Reviewing our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.
- We document our processing activities in electronic form so we can add, remove and amend information easily.

General Controls in Place

- There is a process of continual review to determine whether any changes in the organisation's registration are required as a result of changes in the nature of the business.
- The details of Toynbee Hall are registered are kept up to date.
- The notification to the Information Commissioner's Office is renewed annually.
- Toynbee hall maintains and updates the public data protection register which will be reviewed regularly and at least on an annual basis.

Privacy Notice - Clients, Staff, Donors and Trustees

Toynbee Hall will issue privacy notices from time to time, informing you about the personal information that we collect and hold relating to you, how you can expect your personal information to be used and for what purposes.

We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Individual Rights – Clients, Staff, Donors and Trustees

People have the following rights concerning their personal information:

- To be informed about how, why and on what basis that information is processed.
- To obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request— see the SAR Policy information.
- To have data corrected if it is inaccurate or incomplete;
- To have data erased if it is no longer necessary for the purpose for which it was originally collected / processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten);
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal information, but you require the data to establish, exercise or defend a legal claim; and
- To restrict the processing of personal information temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether the organisation's legitimate grounds override your interests).
- If you wish to exercise any of the rights in the paragraphs above, please contact the data protection officer.

Individual Obligations - Staff and Trustees

Individuals are responsible for helping Toynbee Hall keep their personal information up to date. You should let Toynbee Hall know if the information you have provided to Toynbee Hall changes, for example, if you move to a new house or change details of the bank or building society account to which you are paid.

You may have access to the personal information of other members of staff, suppliers and clients of Toynbee Hall in the course of your employment or engagement. If so, Toynbee Hall expects you to help meet its data protection obligations to those individuals. For example, you should be aware that they may also enjoy the rights set out above.

If you have access to personal information, you must:

- Only access the personal information that you have authority to access, and only for authorised purposes;

- Only allow other Company staff to access personal information if they have appropriate authorisation;

- Only allow individuals who are not Company staff to access personal information if you have specific authority to do so from the data protection officer.

- Keep personal information secure (for example. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in Toynbee Hall's Privacy Policy.

- Not remove personal information, or devices containing personal information (or which can be used to access it), from Toynbee Hall's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and

- Not store personal information on local drives or on personal devices that are used for work purposes.

- You should contact the data protection officer if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

    - Processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions being met;

    - Any data breach as set out below;

    - Access to personal information without the proper authorisation;

    - Personal information not kept or deleted securely;

    - Removal of personal information, or devices containing personal information (or which can be used to access it), from Toynbee Hall's premises
      without appropriate security measures being in place;

- Any other breach of this Policy, or any of the data protection principles set out above.

Information Security

Toynbee Hall will use appropriate technical and organisational measures to keep personal information secure and to protect against unauthorised or unlawful processing and accidental loss, destruction, or damage. These may include:

- Making sure that, where possible, personal information is pseudonymised or encrypted;
- Ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- Ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored promptly; and
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- In rare cases where Toynbee Hall uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:
    - The organisation may act only on the written instructions of Toynbee Hall;
    - Those processing the data are subject to a duty of confidence;
    - Appropriate measures are taken to ensure the security of processing;
    - Sub-contractors are only engaged with the prior consent of Toynbee Hall and under a written contract.
    - The organisation will assist Toynbee Hall in providing subject access and allowing individuals to exercise their rights under the GDPR;
    - The organisation will assist Toynbee Hall in meeting its GDPR obligations concerning the security of processing, the notification of data breaches

and data protection impact assessments;

- The organisation will delete or return all personal information to Toynbee Hall as requested at the end of the contract; and

- Toynbee Hall will submit to audits and inspections, provide Toynbee Hall with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell Toynbee Hall immediately if it is asked to do something infringing data protection law.

- Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the Data Protection Officer.

Storage and Retention of Personal Information – Clients, Staff, Donors and Trustees

- Personal information (and sensitive personal information) will be kept securely following Toynbee Hall's Data Security Policy.

- Personal information (and sensitive personal information) should not be retained any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff should follow Toynbee Hall's Retention Policy which set out the relevant retention period or the criteria that should be used to determine the retention period. Where there is any uncertainty, staff should consult the data protection officer dpo@toynbeehall.org.uk

- Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

Data Breaches

- A data breach may take many different forms, for example:
    - Loss or theft of data or equipment on which personal information is stored;
    - Unauthorised access to or use of personal information either by a member of staff or third-party;
    - Loss of data resulting from an equipment or systems (including hardware and software) failure;
    - Human error, such as accidental deletion or alteration of data;
    - Unforeseen circumstances, such as a fire or flood;
    - Deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
    - 'Blagging' offences, where information is obtained by deceiving the organisation which holds it.
- In the event of a Data Breach, Toynbee Hall will:
    - Make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals;
    - Notify the affected individuals, if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.
    - Risk assesses the situation and determine what steps need to be taken.
    - Immediately take such steps as are necessary to minimise the risk to clients, staff and the organisation.
    - Take such steps as are necessary to ensure that similar breaches cannot happen again.

International Transfer of Data

Toynbee Hall does not intend to transfer personal information outside the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein and Norway) to other countries.

If this were to be required, it would be on the basis that that country, territory or organisation is designated as having an adequate level of protection OR that the organisation receiving the information has provided adequate safeguards by way of standard data protection clauses.

Toynbee Hall's Data Protection Officer should be consulted before any such transfer is made.

Consequences of Failing to Comply

Toynbee Hall takes compliance with this policy very seriously. Failure to comply with the policy:

- Puts at risk the individuals whose personal information is being processed; and
- Carries the risk of significant civil and criminal sanctions for the individual and Toynbee Hall; and
- May, in some circumstances, amount to a criminal offence by the individual.

Because of the importance of this policy, a staff member's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the Data Protection Officer.

Client/Persons Data Storage and Retention

The Directors of managers of Toynbee Hall store personal and sensitive personal information on clients to manage their test results and fulfil the person's unique cases.

Systems Used and Data Stored – Clients

The following core systems are used to store persons/clients' data defined in Clients/Persons data stored.

Access is only provisioned to the staff members who are actively involved in each case and all systems and software access controls are managed internally and by our third-party IT management partners.

- Advice Pro – Case management software
    - Data is stored in the UK within a robust, secure operations centre compliant with the Information Security Code of Practice ISO27001, and automatically backed up daily.
- Upshot – Secure Progress Tracking and Reporting software.
- MAP Tool
- Dotdigital

Systems Used and Data Stored – Staff and Trustee Information

- Cascade and various secure other locations

Systems Used and Data Stored – Donor Information

- Raisers Edge

Other Data Retention

- Microsoft Teams is in use at the organisation and is used for document management and email for business-related activities.

Sharing of Data – Clients/Persons

Client data is only shared when required with the following individuals and organisations:

- Welfare organisations (if required)
- Police and Government related organisations (if required)

Clients Data Stored

Information Type
Client/Persons Data
Data Stored
Personal Information • Contact details including Name, Address, Telephone number/s and email address • Demographic data / Special Category data; Gender, Housing status, Household composition, Ethnicity, Disability and Health, Employment status (all optional with consent). • Client Case Files – details of case and relevant info – correspondence including with 3rd parties. • Client Enquiry Forms, • Advice Line Records, • Client Complaints and feedback. • Data can include financial and in some cases welfare information.
Processing Reason
• Administration of Toynbee Hall services.
Legal Interest/Legitimate Reason
• Legitimate reason for performing contract duties.

• Consent is given by an individual at the initial stage (contract/agreement through consent forms or opt-in on contact forms).
Retention Policy
Please refer to the Data Storage, Retention, Archiving and Destruction section of this document.

Staff and Volunteer Data Stored

Information Type
Staff Data
Data Stored
Personal Information • Name, address, email, telephone number. • Next of Kin. • Application Form data/CV. • Interview notes. • Offer and acceptance letters **Contract** • Dated/signed. • P60/P45. **Photographic Evidence of Identity** • Valid Passport/Driving Licence copy. **Various**

• National Insurance and Bank details. • Copies of relevant qualifications. • Right to Work in the UK • Evidence of Current Address • References. • Training Record. • Record of sickness, leave and disciplinaries. • Statutory Maternity, Adoption, Paternity Pay • Statutory Sick Pay • Payroll and PAYE Records • Health and Safety Consultations • Redundacy Details • Disciplinary, working time and training data
Processing Reason
• Provision of employment obligations. • Fulfilment of contract.
Legal Interest/Legitimate Reason
• Legitimate reason for performing contract duties. • Consent is given by an individual at the initial stage (contract).
Retention Policy
Please refer to the Data Storage, Retention, Archiving and Destruction section of this document.

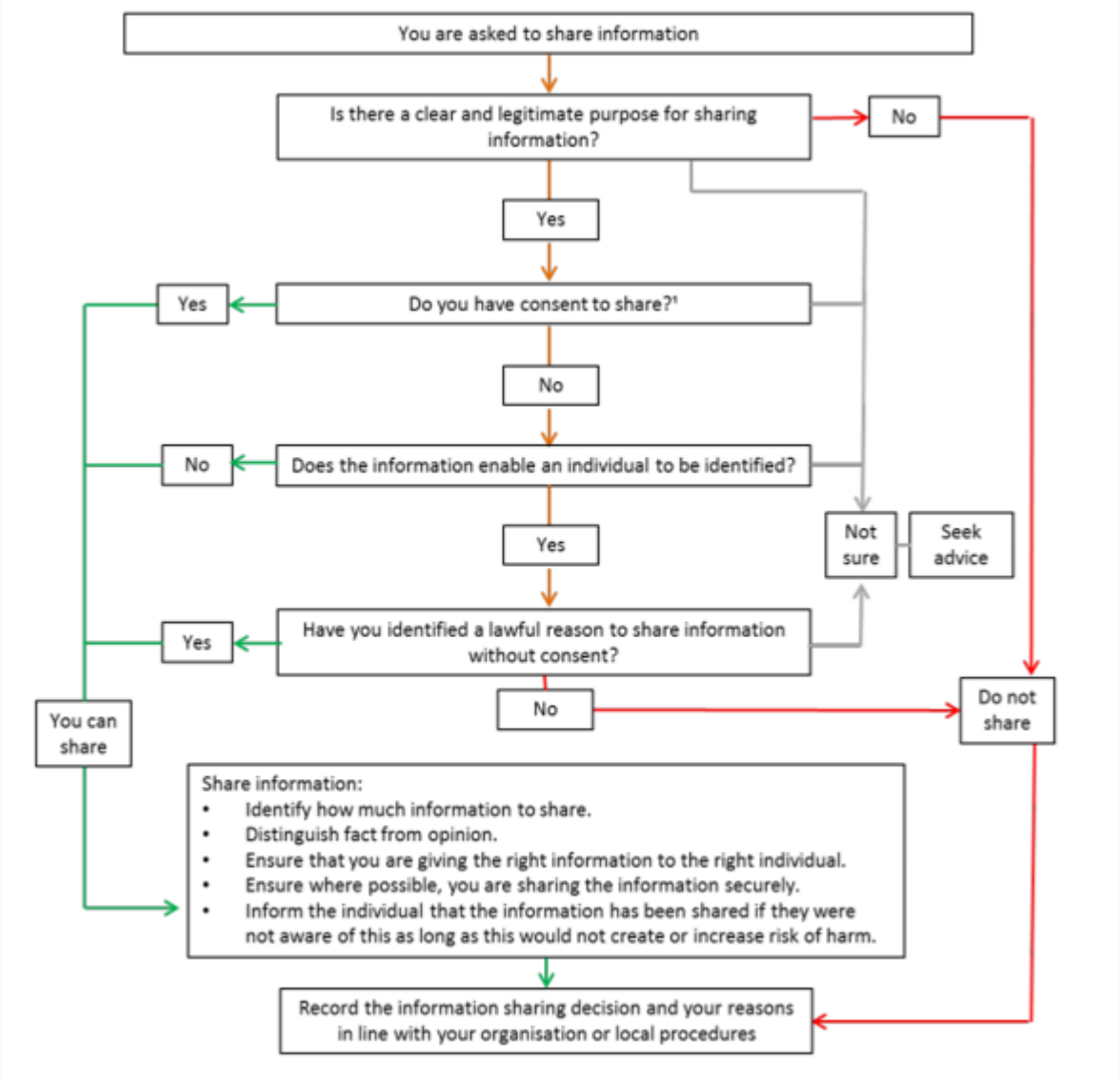
Donor Data Stored

Information Type
Donor Data
Data Stored
• Supporter information, personal details such as name and contact data and amounts contributed.
Processing Reason
• Traceability of supporter finances and marketing
Legal Interest/Legitimate Reason
• Legitimate reason for performing charity duties. • Consent for processing at donation stage.
Retention Policy
Please refer to the Data Storage, Retention, Archiving and Destruction section of this document.

Trustee Data Stored

Information Type
Trustee Data
Data Stored
• Details of Trustees, Director and Management Committee Members. • Board meeting agendas, reports and minutes. • Constitutional Documents, Resolutions and Special Resolutions. • Business Plans,
Processing Reason
• Required for continued management of Toynbee Hall organizational continuity and historical reference.
Legal Interest/Legitimate Reason
• Legitimate reason for performing charity duties.
Retention Policy
Please refer to the Data Storage, Retention, Archiving and Destruction section of this document.

Data Sharing Process Flow – Clients



Subject Access Requests and Data Rights – Clients and Staff

Introduction

Under GDPR legislation, Data Controllers shall provide the information outlined in Articles 13 & 14 to Data Subjects and Data Subjects may access, correct, delete, restrict processing of, and transfer their personal data, as well as object to automated decision-making based on their personal data.

SAR and Data Rights Procedure

Subject Access Requests should come to the email address dpo@toynbeehall.org.uk in the first instance and be followed up with an acknowledgement letter/email.

All requests and their progress must be logged by the data protection officer in a secure place with no external access.

SAR Timescales

All Subject Access Requests will be completed within 30 days unless defined as complex – if the time will exceed 30 days, the requestor will be notified.

SAR Fee's

Subject Access Requests coming directly from the data subject will be free, however, Toynbee Hall can charge a fee if requests become unfounded or excessive. If requests are coming from a client on behalf of a data subject, Toynbee Hall may charge a fee for data retrieval.

SAR Business Processes

The processes cover SAR and other data rights of individuals:

- Right of Access and Data Portability
- Right to Erasure
- Right to Object
- Right to Restriction
- Right to Rectification

Undertaking Privacy Impact Assessments

When Toynbee Hall undertakes the use of new technologies or will be involved in the processing of data that contains a high risk to the rights and freedoms of data subjects, it will undertake a Privacy Impact Assessment.

The scale and nature of each PIA will be shaped on a case-by-case basis, to capture the following information to inform the decision-making process:

- Risk Assessment
- Data types, collection, storage use and deletion methodologies
- Legal basis
- Information flows processes and procedures
- Consultation
- Evaluation of privacy procedures
- Final summary

For further information on PIA Please refer to:

https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Data Storage, Retention, Archiving and Destruction

Retention Statement

Data and records should not be kept for longer than is necessary. This principle finds statutory form in the General Data Protection Regulation (GDPR) 2018 which requires that personal data processed for any purpose "shall not be kept for longer than is necessary for that purpose".

No data file or record should be retained for more than six years after it is closed unless a good reason for longer retention can be demonstrated. It may well be appropriate having regard to the nature of the record to opt for a shorter period.

Reasons for longer retention will include the following:

- The statute requires retention for a longer period
- The record contains information relevant to legal action which has been started or is in contemplation
- Whenever there is a possibility of litigation, the records and information that are likely to be affected should not be amended or disposed of until the threat of litigation has been removed
- The record should be archived for historical or research purposes, e.g., the record relates to important policy development or relates to an event of local or national purpose
- The records are maintained for retrospective comparison
- The records relate to individuals or providers of services who are judged unsatisfactory. The individuals may include employees who have been the subject of serious disciplinary action
- Client cases are deemed as ‘high risk’.

Client Files Archiving and Destruction

Procedure

The end of the client's case administration procedure covers the administrative steps to be taken when a case is closed to ensure that all relevant administrative issues have been completed and that the file is put into storage for the correct period of time.

Toynbee Hall keeps a master log of all closed files, which allow the organisation to keep track of files that become ready for destruction.

- 'High Risk' Cases Definition and Procedure
    - Some case files are deemed to be 'high risk'; if so, these documents must be stored for at least sixteen years after the final entry:
- Any case that has been subject to an insurance claim or other dispute ('other dispute' refers to Toynbee Hall's handling of the case).
- Any case relating to building works or surveyor's reports on the purchase of property or relating to a property.
- Any case which is considered to be substantial, where the sums of money involved are for example in excess of £10,000 or where the advice given was especially complex or where the case is an unusual one.
- In cases concerning mortgage arrears the creditor has up to 12 years to bring a claim against a client before it becomes statute-barred, as part of debt advice we would need to advise clients of this and ideally keep the file to check the advice given if required, and;
- In cases where there is a possibility of litigation in these cases, the adviser should bring the case to the attention of the team manager who should then label the case as 'high risk' and clearly record the disposal date to be sixteen or twelve years after the final entry.

Client Information	
Information	**Retention Period**
Client Case Files	6 years after the last activity on the file (typically payment of bill, closure and archive) except in cases involving a mortgage where the retention period will be 12 years. For clients under the age of 18 the file should be kept for 6 years after the client has turned 18.
Client Enquiry Forms	6 years (unless a full client file was opened in which case in line with that file)
Advice Line Records	6 years (unless a full client file was opened in which case in line with that file)
Client Complaints	6 years (with client file)

Supporter and Donor Information	
Information	**Retention Period**
Supporter records	24 months after the last activity on the file (typically initial consent, a contact or donation) except in potential legacy donor cases or where there is a legitimate interest (ie. duration of redevelopment).
Supporter Complaints	6 years (with client file)

Staff Information	
Information	**Retention Period**
Application forms/interview notes for unsuccessful candidates	12 months
Offer letters and acceptance	Permanently
Disciplinary, working time and training	6 years after employment ceases
Redundancy details	6 years from date of redundancy
Documents proving the right to work in the UK	Two years after employment ceases
Health and safety consultations	Permanently
PAYE Records	4 years
Workplace accidents	3 years after date of last entry. There are specific rules on recording incidents involving hazardous substances.
Payroll	3 years after the end of the tax year they relate to
Statutory maternity, adoption and paternity pay	3 years after the end of the tax year they relate to
Statutory sick pay	3 years after the end of the tax year they relate to
Working time arrangements	2 years from date on which they were made

Trustee Information	
Information	**Retention Period**
Details of Trustees, Directors and Management Committee Members.	6 years after they cease to be members
Board Meeting / Management Committee Meeting Agendas, Reports and Minutes	Permanently for historical purposes
Constitutional documents, Resolutions and Special Resolutions	Permanently
Business Plans	3 years

Destruction and Disposal Statement

All information of a confidential or sensitive nature on paper, card, microfiche, or electronic media must be securely destroyed when it is no longer required. This ensures compliance with the General Data Protection Regulation (UK GDPR) 2018/2021 and the duty of confidentiality we owe to our employees, volunteers, clients and customers.

Destruction and Disposal Procedures

All information, in any format, destroyed from any location must have due regard to confidentiality of our employees, volunteers, clients and customers.

- Confidential data must be disposed of in confidential recycling bins, by commissioned contracted document disposal contractor or in the Toynbee Hall shredders
- All other paper can be disposed of in the boxes or bins provided in offices for environmentally friendly disposal of non-confidential and non-sensitive paper waste.

- The procedure for the destruction of confidential or sensitive waste on electronic media such as tape, disk, cassette/cartridge, hard drives, CD-Rom, DVD and ZIP drive is as follows:
- Media that are being destroyed because they are showing signs of damage or are obsolete should be physically destroyed by being cut into pieces or other ways before disposal
- Destruction of backup copies of such data also needs to be dealt with.

Further details on media information we hold, and the methods used to ensure its protection, security and disposal are set out in the Fundraising and Communication Data Policy and Procedures.

The Confidentiality Policy and Procedures set out the principles as to how Toynbee Hall will ensure confidentiality for staff, volunteers, clients and customers.

The Data Protection Policy set out how the organisation ensures compliance with the General Data Protection Regulation 2018/2021.

Staff Training

Toynbee Hall will ensure that staff are adequately trained regarding their data protection responsibilities.

Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

All members of staff and volunteers are provided with training on Data Protection compliance during their induction and as necessary periodically. Additional training on any changes to this policy and refresher training is provided when required.

All members of staff and volunteers who have access to personal data must comply with this policy and adhere to the procedures laid down by the Data Protection Officer. Failure to comply with this policy by any member of staff or volunteer might result in disciplinary proceedings.

Each staff member and volunteer is responsible for reporting any breach, or suspected breach of this policy.

Governance

This policy and procedure is owned and maintained by the Human Resources Department.

All policies and procedures are reviewed annually by the department responsible; to ensure that we respond to staff needs, business strategy, legislation and any codes of practices determined by the market.