Shoreditch Trust

12 Orsman Road
London N1 5QJ

T 020 7033 8500
www.shoreditchtrust.org.uk

Vat 885423692
Company 03894363
Charity 1086812

DATA PROTECTION POLICY

1 Introduction and Scope

1.1 This policy sets out how the Shoreditch Trust ("we", "our", "us", "the Organisation") handle the personal data of our clients, students, suppliers, partners, employees, volunteers and other third parties.

1.2 This policy is about your obligations under the data protection legislation. Data protection is about regulating the way that the Shoreditch Trust uses and stores information about identifiable people (**Personal Data**). It also gives people various rights regarding their data - such as the right to access the Personal Data that we hold on them. We try to avoid using legal language or jargon in this Policy, however, certain words and phrases have particular meanings under data protection legislation. Please refer to the Glossary at the end for the definitions used in this Policy.

1.3 During the course of our work we will collect, store and process Personal Data about our clients, students, staff, volunteers, the staff of suppliers and other third parties. We recognise that the correct and lawful treatment of this data will maintain confidence in Shoreditch Trust and will ensure that we are compliant with all the relevant legislation.

1.4 We are committed to ensuring that our clients understand the way we use their Personal Data and we want to ensure that their relationship with us is built on mutual trust and transparency. Data protection plays a crucial part in that relationship.

1.5 Data Protection considerations should never be a barrier to sharing safeguarding concerns you have about a client or their family with the Designated Safeguarding Lead.

1.6 The Shoreditch Trust will work with Project Leads to consider and shape the way that the transparency information is best shared with each client group, taking account of their needs.

1.7 This policy is aimed at all Staff working for the Shoreditch Trust (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities ('**you**').

1.8 You are obliged to comply with this policy when processing Personal Data on our behalf. Any breach of this policy may result in disciplinary action.

1.9 This policy does not form part of your contract of employment and may be amended by us at any time.

1.10 Your line manager and the Organisational Support Manager is responsible for helping you to comply with the Trust's obligations. All queries concerning data protection matters should be raised with your line manager and/or the Organisational Support Manager.

2 What information falls within the scope of this policy

Personal Data at work

2.1 In order for you to do your job, you will need to collect, use and create Personal Data. Virtually anything that relates to a living person will include Personal Data.

2.2 Examples of places where Personal Data might be found are:

2.2.1 A report about a safeguarding incident;

2.2.2 An entry in a computer database with contact details;

2.2.3 in a file, such as a client file or referral form;

2.2.4 information on a client's progress through a programme;

2.2.5 an opinion about a client or colleague in an email;

2.2.6 in a register or contract of employment;

2.2.7 letters, attendance notes, meeting minutes and other documents or written records;

2.2.8 health records; and

Categories of Critical Personal Data

2.3 The following categories are referred to as **Critical Personal Data** in this policy You must be particularly careful when dealing with Critical Personal Data which falls into any of the categories below:

2.3.1 Information about safeguarding matters;

2.3.2 Information about physical or mental health or condition - including a special educational need;

2.3.3 racial or ethnic origin;

2.3.4 political opinions;

2.3.5 religious beliefs or other beliefs of a similar nature;

2.3.6 trade union membership;

2.3.7 sex life;

2.3.8 information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved);

2.3.9 genetic or biometric information;

2.3.10 Financial information about colleagues or clients.

If you have any questions about your processing of these categories of Critical Personal Data please speak to the Deputy Chief Executive.

3 The Principles of Data Protection

3.1 We adhere to the Principles relating to Processing of Personal Data set out in the **GDPR** and Data Protection Act 2018 which require Personal Data to be:

3.1.1 Processed lawfully, fairly and in a transparent manner (**Lawfulness, Fairness and Transparency**).

3.1.2 Collected only for specified, explicit and legitimate purposes (**Purpose Limitation**).

3.1.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (**Data Minimisation**).

3.1.4 Accurate and where necessary kept up to date (**Accuracy**).

3.1.5 Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (**Storage Limitation**).

3.1.6 Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (**Security, Integrity and Confidentiality**).

3.1.7 Not transferred to another country without appropriate safeguards being in place (**Transfer Limitation**).

3.1.8 Made available to Data Subjects and Data Subjects allowed to **exercise certain rights in relation to their Personal Data (Data** Subject's Rights and Requests).

3.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (**Accountability**).

4 Your obligations

Personal Data must be processed fairly, lawfully and transparently

4.1 What does this mean in practice?

4.1.1 "Processing" covers virtually everything, which is done in relation to Personal Data, including using, disclosing, copying and storing Personal Data.

4.1.2 People **must** be told what data is collected about them, what it is used for, and who it might be shared with, unless it is obvious. They must also be given other information, such as, what rights they have in their information, how long we keep it for and about their right to complain to the Information Commissioner's Office ("ICO").

4.2 This information is often provided in a document known as a Transparency Notice. Copies of our Transparency/Privacy Notices can be obtained from the Data Protection Folder on Sharepoint or accessed on our website.

4.3 You must familiarise yourself with our Client (arranged per project), Student and Staff Transparency Notices.

4.4 You must only process Personal Data for the following purposes:

4.4.1 as set out in the applicable Transparency/Privacy Notice;

4.4.2 protecting and promoting the Shoreditch Trust's legitimate interests and objectives (for example *ensuring site security, managing safeguarding concerns);* and

4.4.3 to fulfil the Shoreditch Trust's contractual and other legal obligations.

Use of Personal Data

4.5 The Shoreditch Trust maintains an accountability record of all the ways we process personal data, this is reflected in the Transparency Notices. If you want to do something with Personal Data that is new and is not currently on the record, you must speak to the Deputy Chief Executive. This is to make sure that we have a lawful reason for using the Personal Data.

4.6 If you are using Personal Data in a way which you think an individual might think is unfair please speak to the Deputy Chief Executive.

Consent

4.7 We may sometimes rely on the consent of the individual to use their Personal Data. This consent must meet certain requirements and therefore you should speak to the Deputy Chief Executive if you think that you may need to obtain consent.

4.8 Consent is required for certain mail-outs and marketing by electronic means, please check with the Communications Manager before sending any mail-outs to clients or volunteers.

Personal Data must only be processed for limited purposes and in an appropriate way.

4.9 What does this mean in practice?

4.9.1 For example, if employees are told that they will be photographed for the Organisation's website or intranet, you should not use those photographs for another purpose (e.g. in the Organisation's marketing material or social media accounts) **OR** for biographies.

4.9.2 When you are designing a new process or procedure you must take account of the **Privacy by Design** requirements which include undertaking an appropriate **Data Protection Impact Assessment**. When you are planning your changes, please speak to the Project Manager and/or the Deputy Chief Executive for advice and assistance.

Personal Data held must be adequate and relevant for the purpose.

4.10 What does this mean in practice?

4.10.1 This means not making decisions based on incomplete data. For example, when undertaking an employee's appraisal, you must make sure you are using all of the relevant and most up to date information about the employee OR when undertaking a client assessment, you must make sure you are using all of the relevant and most up to date information about the client.

Personal Data must not be excessive or unnecessary.

4.11 What does this mean in practice?

4.11.1 Personal Data must not be processed in a way that is excessive or unnecessary. For example, you should only collect information about an employee's family when it is necessary in relation to work, such as to ensure the Organisation is aware of an employee's next of kin arrangements to in an emergency.

Personal Data that you hold must be accurate.

4.12 What does this mean in practice?

4.12.1 You must ensure that Personal Data is complete and kept up to date. For example, if a client's contact details have changed, you should update the information management system or if you are aware of inaccuracies you must ensure they are updated.

Personal Data must not be kept longer than necessary.

4.13 What does this this mean in practice?

4.13.1 Shoreditch Trust has a record retention policy about how long different types of data should be kept for and when data should be destroyed. This applies to both paper and electronic documents. You must be particularly careful when you are deleting data.

4.13.2 Please speak to the Organisational Support Manager and your line manager for guidance on the retention periods and secure deletion.

Personal Data must be kept secure.

4.14 You must comply with the following Organisation policies and guidance relating to the handling of Personal Data:

4.14.1 Cyber Security Policy;

4.14.2 Staff Handbook;

4.14.3 Information and Records Retention Policy

Personal Data must not be transferred outside the EEA without adequate protection.

4.15 What does this mean in practice?

4.15.1 If you need to transfer personal data outside the EEA please contact the Deputy Chief Executive. For example, if you are sending information to someone outside the EEA in respect of a trip or liaising with an adviser for a client.

5 Sharing Personal Data outside Shoreditch Trust - dos and don'ts

Dos and don'ts: Please review the following dos and don'ts:

5.1 **DO** share Personal Data strictly on a need to know basis - think about why it is necessary to share data outside the Shoreditch Trust - if in doubt - always ask your line manager.

5.2 **DO** share safeguarding concerns with the Designated Safeguarding Lead (The Chief Executive or in Clinical Supervision).

5.3 **DO** encrypt emails, which contain Critical Personal Data. For example, encryption should be used when sending details of an employee's ill health to external advisers or insurers; or payroll details, which are likely to contain several pieces of Critical Personal Data including details to the payroll provider.

5.4 **DO** make sure that you have permission from your line manager and the Communications Manager to share Personal Data on the Organisation website or social media channels.

5.5 **DO** be aware of "blagging". This is the use of deceit to obtain Personal Data from people or organisations. You should seek advice from the Deputy Chief Executive where you are suspicious as to why the information is being requested or if you are unsure of the identity of the requester (e.g. if a request has come from an **existing member but using a different email address).**

5.6 **DO** be aware of phishing. Phishing is a way of making something (such as an email or a letter) appear as if it has come from a trusted source. This is a method used by fraudsters to access valuable personal details, such as usernames and passwords. Don't reply to email, text, or pop-up messages that ask for personal or financial information or click on any links in an email from someone that you don't recognise. Report all concerns about phishing to the Finance Officer and the IT providers.

5.7 **DO NOT** disclose Personal Data to the Police or other statutory agencies such as HMRC or a Local Authority without permission from the Deputy Chief Executive.

5.8 **DO NOT** disclose Personal Data to contractors without permission from the Deputy Chief Executive. This includes, for example, sharing Personal Data with an external marketing team to carry out a marketing campaign.

6 Sharing Personal Data within the Shoreditch Trust

6.1 **Sharing Personal Data:** This section applies when Personal Data is shared within Shoreditch Trust.

6.2 **Need to know basis:** Personal Data must only be shared within Shoreditch Trust on a "need to know" basis.

6.3 **Client files should be locked down to the staff who need to access the information for delivery purposes and wider access granted only to persons with appropriate authority. If you are unsure whether a person has appropriate authority speak to the Deputy Chief Executive.**

6.4 Examples of internal sharing which are **likely** to comply with the GDPR:

6.4.1 liaising with a colleague in HR to check whether a new starter has completed all their induction training;

6.4.2 Speaking to the DSL about concerns for a client or their family;

6.4.3 Making notes of meetings, identifying those who and don't attend.

6.5 Examples of internal sharing which are **unlikely** to comply with the GDPR:

6.5.1 recording an interview or telephone call without the other person knowing;

6.5.2 leaving handover notes that name clients and their specific needs on a colleague's desk while they are away;

6.5.3 using your personal mobile device to take photographs of projects and access work emails without the Shoreditch Trust's consent .

7 Individuals' rights in their Personal Data

7.1 **Rights:** People have various rights in their information. You must be able to recognise when someone is exercising his or her rights so that you can refer the matter to the Deputy Chief Executive.

7.2 **Individual's rights:** Please let the Deputy Chief Executive know if anyone (either for themselves or on behalf of another person, such as a solicitor):

7.2.1 wants to know what information Shoreditch Trust holds about them;

7.2.2 asks to withdraw any consent that they have given to use their information;

7.2.3 wants Shoreditch Trust to delete any information;

7.2.4 asks Shoreditch Trust to correct or change information (unless this is a routine updating of information such as contact details, which falls within your role and authorised access);

7.2.5 asks for electronic information which they provided to Shoreditch Trust to be transferred back to them or to another organisation;

7.2.6 wants Shoreditch Trust to stop using their information for direct marketing purposes. Direct marketing has a broad meaning for data protection purposes and might include communications such as Shoreditch Trust or

7.2.7 objects to how Shoreditch Trust is using their information or wants Shoreditch Trust to stop using their information in a particular way, for example, if they are not happy that information has been shared with a third party.

Requests for Personal Data (Subject Access Requests)

7.3 **The right to request Personal Data:** One of the most commonly exercised rights mentioned in paragraph 7.2 above is the right to make a Subject Access Request. Under this right people are entitled to request a copy of the Personal Data which the Shoreditch Trust holds about them (or in some cases their child) and to certain supplemental information.

7.4 **Form of request:** Subject Access Requests do not have to be labelled as such and do not even have to mention data protection or be in writing. For example, an email which simply states "Please send me copies of all emails you hold about me" is a valid Subject Access Request. As too would a verbal request to any member of staff. **You must always immediately let the Deputy Chief Executive know when you receive any such requests**.

7.5 **If you receive a Subject Access Request:** Receiving a Subject Access Request is a serious matter for Shoreditch Trust and involves complex legal rights. Staff must never respond to a subject access request themselves unless authorised to do so.

7.6 **Disclosure:** When a Subject Access Request is made, Shoreditch Trust must disclose all of that person's Personal Data to them which falls within the scope of the request - there are only very limited exceptions. There is no exemption for embarrassing information - so think carefully when writing letters and emails as they could be disclosed following a Subject Access Request. However, this should not deter you from recording and passing on information to fulfil your professional duties, particularly in relation to money laundering or fraud prevention.

Breach

7.7 **Breach:** A breach of this policy may be treated as misconduct and could result in disciplinary action including in serious cases, dismissal.

7.8 **Criminal Offence:** A member of Staff who deliberately or recklessly misuses or discloses Personal Data held by the Shoreditch Trust without proper authority is also guilty of a criminal offence.

Glossary

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Organisation Personnel and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of **Privacy by Design** and should be conducted for all major system or business change programs involving the Processing of Personal Data.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

General Data Protection Regulation (GDPR): the General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. [Personal Data specifically includes, but is not limited to,

Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

Staff: all employees, workers, contractors, agency workers, consultants, directors, trustees, agency staff, temporary staff, work experience and volunteers and others.

Transparency Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Organisation collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee Transparency Notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

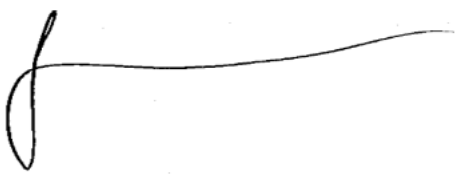
Other Policies and Guidelines

Shoreditch Trust staff and volunteers must refer to the Company Policy folder on Sharepoint for supporting documentation, guidelines and good practice protocols. Please review and ensure you are familiar with company policies and specifically the Cyber Security Policy, Safeguarding Policy and Remote Working Policy.

Approval and Review

This Policy was prepared by the Organisation's lawyers (Veale Wasbrough Vizards LLP) with support and review from the Chief Executive/Safeguarding Lead and the Deputy Chief Executive to provide a framework for the management of its data protection processes and procedures. The policy, along with accompanying documents including the data mapping is reviewed to ensure controls are robust and meet the needs of the business and its client's and staff day to day. The Policy will be reviewed on an annual basis by the Board of Trustees to ensure continuing appropriateness.

Approved by Shoreditch Trust Board
Signed Chair



May 2023
Review date: May 2025