The Worshipful Company of World Traders Charitable Trust

Data Protection Policy

Addressing the General Data Protection Regulation (GDPR) 2018 [EU] and the Data Protection Act (DPA) 2018 [UK]

For information on this Policy or to request Subject Access please contact the Clerk.

Email: clerk@world-traders.org

Phone: 01727 822181

Post: 13 Hall Gardens
Colney Heath
St Albans
Herts
AL4 0QF

Definitions

The Trust holds personal data about our donors, suppliers and other individuals for a variety of business purposes. This policy sets out how we seek to protect personal data and ensure that Officers of the Trustees understand the rules governing their use of personal data to which they have access during their work.

Business purposes	• The purposes for which personal data may be used by us: Meeting the objectives of The Worshipful Company of World Traders Charitable Trust ("the Trust") including monitoring those Members of the Worshipful Company of World Traders ("the Company") who contribute to the Trust, event administration (including the Tacitus lecture) and financial management. • Business purposes include the following*:* • *Compliance with the Trustees legal and governance obligations and good practice* • *Ensuring privacy policies are adhered to (such as policies covering email and internet use)* • *Operational reasons, such as the making of donations to individuals or organisations, recording transactions, event planning and bookings and the distribution of information.* • *Investigating complaints* • *Checking references, ensuring safe working practices, monitoring and managing Trustee and Officer access to administrative information.*
Personal data	Information relating to identifiable individuals, such as current and former donors , , suppliers, those applying for or in receipt of grants from the Trust and livery contacts. Personal data we gather may include: individuals' contact details, bank details (for direct debit purposes) decorations held, education and skills, marital status and job title.
Sensitive personal data	The Trust will not ask for or hold sensitive personal data such as that concerning an individual's racial or ethnic origin, sexual orientation, dietary requirements, political opinions,

religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings.

Scope

This policy applies to all Trustees or officers of the Trust . They must be familiar with this policy and comply with its terms.

This policy supplements any other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be distributed to members.

Who is responsible for this policy?

The Trust is not required to appoint a ***Data Protection Officer.*** The responsibility for this policy rests with the Trustees and is maintained and administered by the Clerk of the Company in the role as Secretary to the Trust and as the Data Processor.

Our procedures

Fair and lawful processing

The Trustees and officers of the Trust must process personal data fairly and lawfully in accordance with individuals' rights. This means that the Trust will only process personal data in accordance with the lawful bases for processing enshrined in the GDPR, primarily legitimate interest, contract or legal obligation. In certain defined circumstances, such as sending personal data outside the UK, the Trustees will only do so if the individual whose details we are processing has consented to the Trustees doing so.

The Data Processing Officer's Responsibilities include

- Keeping the Trustees updated about data protection responsibilities, risks and issues;
- Reviewing all data protection procedures and policies on a regular basis;
- Arranging data protection guidance and advice for all Trustees and Officers of the Trust and all those included in this policy;
- Answering questions on data protection from Members, Court Members and other stakeholders;

- Responding to individuals such as Donors or applicants for grants who wish to know what data is being held on them;
- Checking and approving with third parties that handle the Trust's data any contracts or agreement regarding data processing such as Investment Managers, IT providers and Caterers.

Responsibilities of the Data Processor or his/her Designate

- Ensure all systems, services, software and equipment meet acceptable security standards;
- Checking and scanning security hardware and software regularly to ensure it is functioning properly;
- Researching third-party services, such as cloud services the Trustees are considering using to store or process data;
- Approving data protection statements attached to emails and event notices;

The processing of all data must be:

- Necessary to deliver services to Members of the Company or a third party;
- In the legitimate interests of the Trust and not unduly prejudice the individual's privacy;

The Terms of Business of the Trust include a Privacy Notice ondata protection.

The notice:

- Sets out the purposes for which we hold personal data on individuals;
- Highlights that our work may require us to give information to third parties such as event venues and catering companies;
- Provides that those dealing with the Trust have a right of access to the personal data that the Trust holds about them.

Accuracy and relevance The Trustees will ensure that any personal data they process or is processed on their behalf is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. The Trust will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that the Trust corrects inaccurate personal data relating to them. If an individual believes that information is inaccurate they should record the fact that the accuracy of the information is disputed and inform the Data Processor (the Secretary of the Trust).

Data security

The Trust will keep personal data secure against loss or misuse. Where other organisations process personal data as a service on its behalf, the Secretary will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it;
- Printed data should be shredded when it is no longer needed;
- Data stored on a computer should be protected by strong passwords that are changed regularly;
- Data stored on CDs or memory sticks must be locked away securely when they are not being used;
- The Data Processor must approve any cloud service used to store data;
- Any servers containing personal data must be kept in a secure location, away from general office space;
- Data should be regularly backed up in line with the Trusts' backup procedures;
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones;
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data retention

The Trust will not retain personal data for longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reasons that the personal data was obtained but should be determined in a manner consistent with its data retention guidelines.

Data audit and register

An annual data audit to manage and mitigate risks will inform the data register. This should contain information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Subject access requests

Under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them. This requirement is included in the GDPR 2018 and is also included in the DPA 2018 Act.

All subject access requests should be referred immediately to the Secretary (Data Processor).

Processing data in accordance with the individual's rights

The Trust will abide by any request from an individual not to use their personal data for direct marketing purposes and notify the Clerk as Secretary to the Trust about any such request. The Trust will not send direct marketing material to someone electronically (e.g. via email) unless it has an existing relationship with them regarding the service or event being marketed.

The Trust does not give, sell or allow personal data to be used by any third party for marketing purposes..

Training

The Secretary of the Trust and the Chairman have received training on this policy. Further training will be obtained whenever there is a substantial change in the law or our policy and procedure.

Training covered:

- The law relating to data protection
- Related policies and procedures.

Revised Policy approved by the Trustees on 21 September 2020.