The Worshipful Company of Broderers

and Broderers' Charity Trust

Data Protection Policy

Addressing the General Data Protection Regulation (GDPR) (Reg [EU] 2016/679) and the Data Protection Act (DPA) 2018 [UK]

INTRODUCTION

1. The Worshipful Company of Broderers and Broderers' Charity Trust (hereinafter referred to as 'the Company') hold personal data about its employees, Members, suppliers and other individuals for a variety of business purposes. This policy sets out how the Company seeks to protect personal data and ensure that Officers, Members and staff understand the rules governing their use of personal data to which they have access in the course of their work.

DEFINITIONS

2. **Business Purposes**. The broad purposes for which personal data may be used by the Company:

- Membership management.
- Event administration.
- Financial management.

Business purposes include the following:

- Compliance with legal, regulatory and governance obligations and good practice.
- Ensuring business policies are adhered to (such as policies covering email and internet use).
- Operational reasons, such as recording transactions, event planning, bookings, distribution of information and merchandise.
- Collection of donations and subscriptions.
- Investigating complaints
- Checking references, ensuring safe working practices, monitoring and managing Officer access to administrative information.
- Improving service to and support of Members.

3. **Personal Data**. Information relating to identifiable individuals, such as Freedom applicants, current and former Members, employed and contracted staff and Officers, suppliers and Livery contacts. Personal data gathered by the Company may include: individuals' contact details; marital status and family details; educational and occupational background; details of certificates, diplomas, honours & awards held; job title, and short CV (see Annex A for full list).

4. **Sensitive Personal Data**. Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences or related proceedings is not sought or held by the Company. Where Members' and guests' dietary or health requirements are made known to the Company steps will be taken to ensure that 3rd parties with whom this must, necessarily, be shared (e.g. Livery Halls and Catering Establishments) have made an undertaking to delete the data on completion of the event for which the information was provided.

SCOPE

5. This policy applies to all Officers, Trustees and staff of the Company, who must be familiar with this policy and comply with its terms and supplements and with any other policies relating to internet and email use. The Company 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.

RESPONSIBILTIY

6. Given the low level of data held, the Court have determined that a Data Protection Officer is not required[1]. The Company Officers in any year are the Company's Data Controllers; responsibility for this policy lies with the Court and is maintained and administered by the Clerk as the Data Processor.

PROCEDURES

7. **Fair and lawful processing**. The Company must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that personal data is not processed without the individual's consent.

8. **The Data Processor's responsibilities**:

- Keeping the Court updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and policies on a regular basis.
- As needed, arranging data protection guidance and advice for Court members and those included in this policy.
- Answering questions on data protection from Members and other stakeholders.
- Responding to Members and suppliers who may wish to know what data is being held on them by the Company.
- Checking and approving with third parties (such as caterers) that handle the Company's data any contracts or agreement regarding data processing.
- Ensuring all systems, services, software and equipment meet acceptable security standards.
- Checking and scanning security hardware and software regularly to ensure it is functioning properly.

[1] Court Meeting 6th March 2018.

- Researching third-party services, such as cloud services the company may consider using to store or process data.
- Approving data protection statements attached to emails and event notices.

9. **Data Processing**. The processing of all data must be

- Necessary to deliver services to the Members.
- In the Company's legitimate interests and not must not unduly prejudice the individual's privacy. (In most cases this provision will apply to routine business data processing activities.)
- Conducted in compliance with the principles of data protection.[2]
- Subject to the active consent by the data subject; this consent can be revoked at any time.

10. **Privacy Notice**. The Company's Terms of Business include a Privacy Notice to Members on data protection (see Annex A) which:

- Sets out the purposes for which we hold personal data on Members.
- Highlights that Company business may require information to be given to third parties such as Livery Halls, other venues and catering companies.
- Provides that Members have a right of access to the personal data held about them.

11. **Accuracy and Relevance**. The Company will ensure that any personal data it processes is accurate, adequate, relevant and is not excessive, given the purpose for which it was obtained. Data obtained for one purpose will not be processed for any unconnected purpose unless the individual concerned has agreed or would otherwise reasonably expect this to happen. Individuals may ask that the Company corrects inaccurate personal data relating to them. If a Members believes that information is inaccurate they should record the fact that the accuracy of the information is disputed and inform the Clerk, as the Data Processor.

12. **Individuals' Personal Data**. Members must take reasonable steps to ensure that personal data held by the Company about them is accurate and updated as required. For example, if personal circumstances change, the Clerk should be informed so that records can be updated.

13. **Data Security**. Personal data must be kept secure against loss or misuse. If other organisations process personal data as a service on the Company's behalf, the Clerk will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

14. **Secure Data Storage**.

- When data is stored on printed paper, it should be kept in a secure place where it cannot be accessed by unauthorised personnel.
- 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 not being used.

[2] The 8 principles of data protection are detailed at: https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/

- The Clerk must approve any cloud service used to store data.
- 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 Company's backup procedures.
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.
- Any servers containing sensitive data must be approved and protected by security software and a strong firewall.

15. **Data Retention**. The Company must not retain personal data for longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

16. **Data Portability / Subject Access Requests (SAR)**. Under the DPA (1998) and GDPR individuals are entitled, subject to certain exceptions, to request access to information held about them; this requirement is expected to be included in the DPA (2018). Members requesting such information are to use the procedure at Annex B and direct the SAR to the Clerk (Data Processor). This information will be provided without charge; without delay and within one month. If an extension is required, or requests are considered manifestly unfounded or excessive, in particular because they are repetitive, the Company may choose to charge a reasonable fee, taking into account the administrative costs of providing the information, or it may refuse to respond. The reasons for this will be formally notified to you and your right to appeal to the appropriate Supervisory Authority (the UK Information Commissioner's Office) will be highlighted.

17. **Right to be Forgotten**. Any Member may request that any information held on them is deleted or removed; any third party who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies; Members should note that records of the Company's membership are held for historical purposes, both within the Company and at Guildhall.

18. **Processing Data in Accordance with the Individual's Rights**. The Company does not use personal data for third party marketing but does forward information about City events and activities that might be of interest to the Livery; however, it will abide by any specific request from an individual not to use their personal data for such purposes.

19. **Training**. The Clerk has received training on this policy, through a Livery Committee seminar and subject courses; further training will be obtained whenever there is a substantial change in the law, of in the Company's policy or procedures. Court Officers have been briefed on their responsibilities as Data Controllers.

20. **Privacy by Design and Default**. Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. The Data Processor (Clerk) will be responsible for conducting Privacy Impact Assessments and ensuring that any IT projects commence with a privacy plan. When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

21. **International Data Transfers**. No data may be transferred outside the EEA without first discussing it with the Clerk (Data Processor). Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

22. **Data Audit and Register**. Regular data audits to manage and mitigate risks will inform the data register, this contains 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.

23. **Reporting Breaches**. All Officers have an obligation to report actual or potential data protection compliance failures. This allows the Company to:

- Investigate a failure and take remedial steps if necessary.
- Maintain a register of compliance failures.
- Notify the Information Commissioner's Office (ICO) of any compliance failures that are material either in their own right or as part of a pattern of failures.

24. **Monitoring**. Everyone is obliged to observe this policy. The Data Processor (Clerk) has overall responsibility for this policy and will monitor it regularly to ensure adherence.

25. **Consequences of Failure to Comply**. The Company takes compliance with this policy very seriously. Failure to comply puts Members and the Company at risk; any questions or concerns should be addressed, in the first instance, to the Data Processor (the Clerk).

The Clerk 01 May 2018

Annexes:

A. Privacy Notice.
B Subject Access Request.