Definitions

The Company holds personal data about our employees, members, 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 Company understand the rules governing their use of personal data to which they have access in the course of their work.

This Data Protection Policy should be read in conjunction with any separate privacy notice that may have been provided to you.

Business purposes

The purposes for which personal data may be used by us:

- *Membership management, event administration and financial management.*
- *Business purposes including the following:*
  - *Compliance with our 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 recording transactions, event planning and bookings, distribution of information and merchandise.*
  - *Investigating complaints*
  - *Checking references, ensuring safe working practices, monitoring and managing Officer access to administrative information.*
  - *Promoting our craft trade*
  - *Improving services to members*

Personal data

Information relating to identifiable individuals, such as freedom applicants, current and former members, self-employed and other officers, suppliers and livery contacts.

Personal data we gather may include: individuals' contact details, educational background, details of qualification certificates and diplomas, decorations held, education and skills, marital status and job title. It may also include photographs or images as described below.

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.

Sensitive personal data about individuals is collected and used in limited circumstances only, as described below. Sensitive personal data about an individual will never be collected or used without the individual's explicit consent and a clear explanation as to why it is required.

Scope

This policy applies to all officers of the Company and Trustees of Company's Charities. You 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 made available to members via the Company's website (or in hard copy form if requested).

Who is responsible for this policy?

The Company is not required to appoint a Data Protection Officer. The responsibility for this policy rests with the Court and is maintained and administered by the Clerk.

Our procedures

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to us doing so.

The Clerk's responsibilities

- Keeping the Court 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 Court members and those included in this policy
- Answering questions on data protection from Members, Court Members and other stakeholders
- Responding to individuals such as Members and Suppliers who wish to know what data is being held on them by the Company
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing such as IT providers and Caterers.
- Ensuring that 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 company is 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 our Members
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine Membership and Event data processing activities.

Privacy notices

The Company's procedures include issuing Privacy Notices to Members and others on data protection. Privacy Notices:

- Set out the purposes for which we hold personal data on Members, Officers and others
- Highlight that our work may require us to give information to third parties such as event venues and catering companies
- Provide that customers have a right to request access to the personal data that we hold about them

The Company's Data Protection Policy and any Privacy Notice(s) issued to Members form part of the Terms and Conditions for being a member of the Company.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We 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 we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the Clerk.

Your personal data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Clerk so that the data can be updated in the records.

Sensitive personal data

The Company does not routinely collect, hold or use sensitive personal data. Sensitive personal data about an individual will not be collected or used without the individual's explicit consent and a clear explanation as to why it is required. Examples of this data include:

- Dietary Requirements which will be required by the caterers at an event to be attended by the individual.
- Medical conditions that organisers of events need to be aware of for the individual's safety at an event.

Photographs

Photographs or videos taken at Company events are personal data. They may be used on the Company's website and social media, or in the Company's newsletters or promotional material. Photographs may also be displayed in online galleries of official event photographers in order to enable members and guests to download or order copies as personal mementos of events attended.

Data security

We will keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the Clerk 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 will be kept in a secure place where unauthorised personnel cannot access it
- Printed data will be shredded when it is no longer needed
- Data stored on a computer will be protected by strong passwords that are changed regularly.
- Data stored on CDs or memory sticks will be locked away securely when they are not being used
- The Clerk must approve any cloud service used to store data
- Any servers containing personal data will be kept in a secure location, away from general office space
- Data will be regularly backed up in line with the company's backup procedures
- Data will 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

We will 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 will be determined in a manner consistent with our data retention guidelines.

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 expected to be included in the new Data Protection Act which is currently before Parliament (replacing the Data Protection Act 1998).

Subject access requests should be referred immediately to the Clerk.

Please contact the Clerk if you would like to correct or request information that we hold about you. There are restrictions on the information to which you are entitled under applicable law.

Processing data in accordance with the individual's rights

We will abide by any request from an individual not to use their personal data for direct marketing purposes and the Clerk will be notified of any such request.

We will not send direct marketing material to someone electronically (e.g. via email) unless we have an existing business relationship with them in relation to the services being marketed.

Training

The Clerk has 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 has been provided through a Livery Committee seminar and subject courses.

Training covered:

- The law relating to data protection
- Our data protection and related policies and procedures.

GDPR 2018 provisions

Where not specified previously in this policy, the following provisions will be in effect on or before 25 May 2018.

Privacy Notice - transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important to the Company. The following are details on how we collect data and what we will do with it:

What information is being collected?	Full name, address, age, telephone and email contacts, professional experience, facial photo, interests as they relate to Company activities, any diet requests, aspiration to join the Court
Who is collecting it?	The Clerk to the Company
How is it collected?	Freedom and Livery applications, Event bookings, Surveys
Why is it being collected?	To Process Applications, arrange admissions and clothings, establish accurate event arrangements, to learn of members interests and aspirations
How will it be used?	Maintain a database, generate address labels and letters, prepare ceremonies, book dinner numbers and request diets.
Who will it be shared with?	Within the Company; the Membership Committee and the Court. Outside the Company with the City Electoral register and the City Bluebook Directory but only with members' permission.
Identity and contact details of any data controllers	The Clerk is the sole administrator. His contact telephone number is 01455 203152, or email clerk@frameworkknitters.co.uk. The Honorary Treasurer monitors receipts from and payments to Members. His contact email is treasurer@frameworkknitters.co.uk
Details of transfers to third country and safeguards	No information is transferred to a foreign country.
Retention period	Names, contact details and relevant Company admission, resignation and death dates are maintained in the database as a historical record of the Company's members.

Conditions for processing

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All Officers who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Justification for processing personal data

We will process personal data in compliance with all six data protection principles.

Consent

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

Data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The Clerk will be responsible for conducting Privacy Impact Assessments and ensuring that all 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.

International data transfers

The Company will not transfer personal data outside the EEA. If for any reason there is a need to transfer personal data outside the EEA, the Clerk must be consulted and specific consent from the data subject must be obtained prior to the transfer.

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.

Reporting breaches

All Officers have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the 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.

Please refer to our Compliance Failure Policy for our reporting procedure.

Monitoring

Everyone must observe this policy. The Clerk has overall responsibility for this policy. He/she will monitor it regularly to make sure it is being adhered to.

Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the Company at risk.

Data subjects have rights to complain to the Data Protection Regulator (currently the ICO) if the requirements of the GDPR and/or other data protection regulations ae not adhered to.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action. If you have any questions or concerns about this policy, contact the the Clerk.