* 1. **Data Protection & Information Security**:

 The Grand Council of Knight Masons recognises that the safety and security of its voluntary administrators, data systems and members is of paramount importance and is essential for the Grand Council of Knight Masons to satisfy its obligations under the General Data Protection Regulations (GDPR) and Data Protection Act 2018. The objective of the policy is to ensure that all members and volunteers understand their responsibilities when processing personal data and that methods of handling that information are clearly understood. Individuals are also assured that their personal data is processed in accordance with the data protection principles, that their data is secure at all times and safe from unauthorised access, alteration, use or loss.

* + 1. **Data Protection Principles and Data Subject Rights:**

The GDPR is based on the following principles: All personal data must be:

1. Processed fairly, lawfully and in a transparent manner in relation to the data subject 2. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with these purposes.

3. Adequate, relevant and limited to what is necessary in relation to purposes for which they are processed

4. Accurate and where necessary kept up to date

5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

6. Processed in a way that ensures appropriate security of the personal data including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures The 7th principle holds the Data Controller and the Data Processor accountable for ensuring compliance with the above principles.

Rights of Data Subjects The GDPR sets out the following rights in relation to data subjects:

1. The right to be informed

2. The right of access

3. The right to rectification

4. The right to erasure

5. The right to restrict processing

6. The right to data portability

7. The right to object

8. Rights with respect to automated decision making and profiling Principles of Data Protection Before processing any personal data, all employees, directors and volunteers should consider the following:

• Do we require the information?

• Does the information include special categories of data? This includes: o Race o Ethnic Origin o Political Beliefs o Religious Beliefs o Trade Union Membership o Health Data o Sexual Orientation o Genetic Data 59 o Biometric Data • Has the individual been told that this type of data will be processed?

• Are you authorised to collect/store/process the data?

• If yes, have you checked with the data subject that the data is accurate?

• Are you sure that the data is secure?

• If you do not have the data subject’s consent to process, are you satisfied that it is in the best interests of the individual or the safety of others to collect and retain the data?

Subject Access Requests GDPR gives data subjects the right of access to data. A request for personal data is a Subject Access Request (SAR). A SAR must be made in writing to the Data Protection Officer. A response to a SAR must be acknowledged within 7 days and must be responded to within 30 calendar days of the date of receipt of the request. Routine requests should be dealt with more immediately. Information requests should always be dealt with in a courteous manner.

On submission of a SAR, the data subject is entitled to:

• Be told that personal data about them is being held/is not held

• Be given a description of the personal data and the purpose(s) for which the data is being held. Individuals whose images are recorded have a right to view the images of themselves and, unless they agree otherwise, to be provided with a copy of the images. If images of third parties are also shown with the images of the person who has made the access request, you must consider whether you need to obscure the images of third parties. If providing these images would involve an unfair intrusion into the privacy of the third party, or cause unwarranted harm or distress, then they should be obscured. In all cases when a SAR is received you must be sure the person is who they say they are before any information is released. The personal data disclosed should normally be that which is held at the time the request is made. Data must not be tampered with in any way in order to make it acceptable to the applicant. Some personal data may be exempt from disclosure or legitimately withheld when responding to a SAR (Exemptions). The data should be provided in a legible format and in a permanent form. Authorisation to respond to a Subject Access Request Internal requests received for personal information from membership may be dealt with by the Compliance Officer.

Any other Subject Access Requests must be dealt with by the Data Protection Officer. If you are in any doubt regarding the release of information please refer to the Data Protection Officer for advice and guidance.

1.1.2 **Computer Systems** of Grand Council of Knight Masons recognises the potential threat to membership security and business if stored information is lost or stolen through system security being compromised and will implement the following measures to mitigate this risk. • All electronic information outwith the member database is stored on secure encrypted UK-based cloud server solution. Network security is protected through the use of firewalls and encrypted transmission.

 The Business Continuity Plan contains contingency plans in the event of data being compromised or equipment or system failure. Minimal paper records (relating to accounting and application forms are stored for the minimum period in a locked storage area for the current and previous financial year. • Staff and volunteers who require it to facilitate them carrying out their duties. Access to the relevant area of storage will be approved by the Great Chief’s Cabinet. The Grand Scribe will have access to the network will only be given to those members and volunteers who have been identified as requiring doing so to facilitate the carrying on of their duties and only then under the scrutiny of the network provider. Access to the network will be approved by the Grand Scribe or Compliance Officer. All work carried out remotely by authorised members and volunteers will be through Grand Council of Knight Masons configured laptop, accessing network drives only and using assigned log in credentials and multi factor authentication (MFA). Under no circumstances will personal devices be used for the purposes of remote access or any data be saved to drives on personal devices such as laptops, hard drives or USB flash drives.

1.1.3 **Software Maintenance**: Software maintenance is to be carried out by and the reconised IT services provider only in compliance with the extant maintenance contracts. No member of member or volunteer will load unauthorised software on any computer or laptop. Authorised software can only be loaded under the control of the appropriate IT maintenance person using the Administrator username and password.

1.1.4 **Access Authorisation**: In carrying out its business, the membership and volunteers of the Grand Council of Knight Masons are required to collect, process and access the personal details of its members. It also creates and retains **Members Name**, **Date of Joining a Subordinate Council of Knight Masons**, **Name of Subordinate Council**, **email address** or **Postal address** where required. In order to process this information and create files and documents, Subordinate Council Scribes are required to forward the information to the Grand Scribe to update the membership records. Access to the Grand Council of Knight Masons computer system will be restricted on the basis of the need of the individual member, or volunteer in the performance of their role within the Grand Council administration and authorised by the Great Chief’s Cabinet • The Great Chief, The Grand Scribe, the Deputy Grand Scribe, the Assistant Great Chief, the Grand Treasurer, the Assistant Grand Treasurer.

1.1.5 **Accessing the Computer System**: No person shall use a Grand Council of Knight Masons laptop or desktop computer unless they have been authorised to do so and can demonstrate their competence to use the machinery. Grand Council computers will be used for Grand Council business only. When using the Grand Council’s computer system, only authorised persons are permitted to log on to the system using a unique username and password. Passwords should be of sufficient strength and not include such words as your name, the name of any children; the company name, your date of birth or the word password. Computer systems are set to allow only the Grand Scribe to log in using their own log in credentials when not using their own computer. Unique username and log in passwords must not be divulged to other staff members and should be changed regularly and immediately when prompted to do so. All computers should be locked when left unattended and should be fully closed down when not in use.

1.1.6 **Processing / Viewing Data**: It is the responsibility of all staff and volunteers of Grand Council of Knight Masons to ensure that any personal data they have responsibility for is protected. By taking simple security steps the risks of any personal data being compromised is reduced significantly.

• Staff must ensure that when dealing with members within the Grand Council office, the only documentation on view is that of the member they are dealing with at the time.

• All filing cabinets containing personal information will be locked at all times unless in use.

• All documentation containing personal data will be stored securely within the appropriate filing cabinet or desk drawer.

• When viewing data, the computer must not be left open if you require leaving the workstation unattended. If a workstation must be left unattended, the screen must be locked or if for a prolonged absence logged off before doing so.

• Care must be taken to ensure that members cannot view data that does not relate to them.

• Computer screens should not be visible from an external source such as a window and where this is not possible action will be taken to ensure visibility is obscured.

• No disk, flash drive or other peripheral shall be inserted into any workstation • All persons using the computer system shall comply with the rules of the General Data Protection Regulations (GDPR) and the Data Protection Act 2018.

1.1.7 **Document Security**: All confidential waste will be destroyed on-site at Grand Council of Knight Masons premises using a mobile shredding Unit.

 1.1.8 **Data Breaches**: Any compromise of the integrity of any personal information by staff or volunteers must be reported to the Grand Scribe who will in turn inform the Data Protection Officer (DPO) *(if required)* . The DPO will: • Assess the risk posed by the breach – use guidance provided by the Information Commissioner’s Office (ICO) • Determine the cause of the breach and any relevant steps required to prevent any recurrence, including potential staff training or process changes • Determine, based on risk, who, if anyone, needs to be notified of the breach (data subjects, ICO etc) • Ensure compliance with all relevant timeframes including 72 hour reporting to ICO timeframe • Record all breaches, regardless of size or impact, on the Grand Council’s breach log and save relevant supporting documentation. Failure to adhere to the requirements of this policy and any data breaches or breaches of confidentiality not covered by law will be dealt with under the Great Chief’s Cabinet.

1.1.9 **Office Security Key Holders**: Access to Grand Council of Knight Masons offices, outside business hours is restricted, with only identified individuals holding a key. A full list of key holders will be held by the Grand Scribe.

• Staff and volunteers within the Grand Council offices will ensure that all external and internal security doors are closed and secure at all times and no unauthorised access can be gained.

• All visitors to Grand Council offices will be accompanied by a member of the Great Chief’s Cabinet or nominated volunteer at all times within the Grand Council offices • When closing the staff or volunteers will ensure that all windows and internal and external security doors are locked.