Visiting Volunteers Data Protection Guidance

Background

The Data Protection Act 2018 ("the Act") establishes a framework of rights and duties which are designed to safeguard the right to privacy with respect to the processing of personal data[1].

The Masonic Charitable Foundation ("the Foundation") (Registered charity number 1164703, Company number 09751836) is committed to protecting the rights of individuals in accordance with the provisions of the Act. For further information visit ico.gov.uk

Purpose of Guidance

This Guidance sets out your responsibilities as a Visiting Volunteer and must be read in full. The guidance must be followed as failing to comply with the Act could result in embarrassment for the individuals we seek to help, damage to the reputation of the Foundation, and Freemasonry. In serious cases it can have significant legal implications and the Foundation may incur a costly fine.

If you have any questions about your responsibilities or any part of the Guidance then please contact the Visiting Volunteer Team.

Important Terms

Data Controller	The organisation that determines how and why personal data will be used.
Data Processor	An organisation or individual, who is not an employee, which processes personal data on behalf of a data controller. This does NOT include volunteers.
Data Subject	An individual who is the subject of personal data. For

[1] Enforcement of the GDPR commences on 25 May 2018 .

	example, an individual applying to the Foundation for support.
Personal Data	Any information relating to an identified or identifiable natural person. It includes, for example, name, date of birth, and opinions about the individual.
Processing	Any use to which personal data are put, including: • Obtaining and retrieving • Holding and storing • Making available to others within or outside the organisation (including sending by email) • Printing, storing, matching, comparing, destroying
Sensitive Personal Data	Defined as information consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, Trade Union Membership, genetic data, biometric data, data concerning health, sex life or sexual orientation.
The Information Commissioner's Office (ICO)	The UK's independent public authority set up to uphold information rights. It is responsible for data protection in England, Scotland, Wales and Northern Ireland and enforces and oversees legislation including the Data Protection Act.

Key principles of Data Protection

- Data is processed lawfully, fairly and in a transparent manner
- Data is obtained for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Data processed is adequate, relevant and limited to what is necessary
- Data is accurate and, where necessary kept up to date
- Data is kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data are processed
- Data processed in accordance with the data subjects' rights

- Data processed in a way that ensures appropriate security of the personal data
- Data not to be transferred to a third country or to an international organization if the provisions of the Regulations are not complied with.

What does this mean in practice?

Responsibilities of the Visiting Volunteer (“You”)

- You must only act on instructions issued by the Foundation
- You must follow the guidance set out in this document and given during any training sessions
- You must take appropriate steps to maintain confidentiality
- You must implement appropriate security measures to protect personal and sensitive personal data
- You must report any breaches to the Masonic Charitable Foundation without undue delay

What to do in the event of a breach

- You must inform the Foundation immediately of incidents where personal data may have been lost, stolen, viewed by or disclosed to unauthorised individuals by contacting the MCF's Data Protection Officer.
- You must take immediate steps to prevent further incidents, for example by changing passwords and locks.

Guidance on complying

The following sets out steps you must take to ensure you comply with Data Protection legislation.

General

- Always care for other people's personal data in the same way that you would want anyone else to care for yours.
- Maintain confidentiality: do not disclose personal information to anyone who is not authorised to receive that information either during your time as a volunteer or after. If in doubt, check with a representative of the Masonic Charitable Foundation. Confidential information is any information that is not available to the public in general.
- Before you give out information over the phone verify who you are talking to. Remember some people may wish to trick you. Ask the caller to give their full name and information specific to their application before disclosing any personal data. If you are not comfortable, ask more questions or call the person back using the contact information you hold.
- Only collect the information you need for the application process.

- Be clear that you are collecting the information on behalf of the Foundation and direct people to the Fair Collection Statement at https://mcf.org.uk/privacy-enquiries-applications-grants/ for details of how their information will be used.
    - The personal data and information you collect must only be used for making an application to the Foundation. You must not keep or use it for any other reason without the explicit consent of the individual concerned. For example you must not use the information provided to make an application to a Provincial charity unless the applicant has given their explicit permission for you to do this.
    - Ensure that any personal and sensitive personal data provided to the Foundation is accurate and up-to-date. Notify the Foundation immediately of any changes or errors.
    - Avoid recording personal opinions not based on fact about the applicant and/or any other individual. The individual concerned has the right to see your comments so you should never write anything that you would not wish them to see.

- If someone asks for a copy of the information the MCF holds on them, you must notify the Visiting Volunteer team immediately so that they can respond to the request.

Storing and disposing of data

- Ensure that all manual files are securely stored out of sight and locked away. Personal and sensitive personal data must not be accessible to anyone who has not signed the declaration on the application form and/or who is not directly involved in the application. This includes the wives, partners and family members of Visiting Volunteers.
- Do not keep personal data for any longer than it is needed. All application forms and supporting materials must be submitted to the Foundation or securely destroyed. Copies of applications must not be retained following confirmation of receipt of the application. Administrative records must be restricted to the minimum information required to carry out your role as a Visiting Volunteer.
- Destroy files and information using a confidential method, such as shredding, for manual records. Electronic files must be permanently deleted.

Electronic security

- Take all reasonable precautions to ensure the confidentiality of personal and sensitive personal data stored on computers, laptops or other electronic devices, or transmitted via email.
- Do not access confidential information using public or open wifi connections.
- Install firewalls and antivirus software on computers and download the latest patches or updates on a regular basis.
- Passwords protect computers, memory sticks, equivalent devices and files. Use strong passwords containing a mix of upper and lower case letters, numbers and symbols. Where possible use encryption when storing or transmitting data that would cause damage or distress if it were lost or stolen.
- Never disclose your passwords to anyone. Do not use autocomplete or ‘remember me’ when entering passwords.

Email

- Ensure your email account can only be accessed by you. Do not use a joint email account. Visiting Volunteers should consider opening an email account specifically for their Visiting Volunteer activities.
- Be aware of the risks associated with junk and spam emails. Email attachments can carry viruses and appropriate antivirus software should be used to scan attachments to ensure they are safe to open. If in doubt it is always best not to open the attachment.
- Emails must not be retained indefinitely, including in archive and deleted items folders. All emails relating to a case must be deleted once notification of the outcome of the application is received.
- When typing the name of the recipient into an email, be careful to choose the right address if the autocomplete function suggests several choices.
- Use the BCC function when sending group emails, unless you have the consent of the recipients to share their email addresses with one another.
- When sending a password protected document, ensure that the password is transmitted under separate cover.
- Do not store data on mobile devices. Password protect 'smart' devices and enable remote deletion to prevent access to, for example, email accounts.

Accidental disclosure, loss and destruction of personal data

- Take all reasonable steps to prevent accidental loss, disclosure or destruction of personal data.
- In public places, take sensible steps to prevent the loss or theft of manual files and electronic equipment.
- Address all mail to a named recipient, seal the envelope securely and mark it 'Confidential – for addressee only'. Ensure appropriate postage is always applied.
- Avoid giving personal data by telephone unless you are certain that the caller is the person he/she claims to be, and is an appropriate person to receive the data.

Last reviewed / updated August 2018

Next review / update due: August 2019