Security of our systems

1. Our database

We use a market leading database for all the personal and contact information we hold about people with whom we have contact. This is called The Raisers Edge and is provided by Blackbaud, who are a market leader in database management. Your data is hosted by Blackbaud in Boston, Massachusetts which explains the Privacy Shield & Safe Harbour Agreement Blackbaud has in place to comply with the EU-US Privacy Shield Framework.

Only staff can access the database, once they have been authorised and are set up to do so. Their only access point is via their work-issued laptop which is password protected (see below) and then through a Citrix receiver. This citrix platform provides further security and requires an individual user name and second password for access.

2. Our office IT system

A substantial amount of our IT provision is managed by a Third-party company, OGL. OGL comply with the market standards for IT provision, ISO 9001:2008 & ISO 27001:2013 please see **Appendix 9a.**

We have a shared server on which we store working documents and information we require to operate our business. OGL monitor our server and provide a market leading firewall, Watchguard, see **Appendix 9b** The Watchguard provides the very latest proactive data protection. Our server is password protected and can only be accessed by two authorised staff members.

Staff can only access the server via their work issues laptop. These laptops are individually protected by 14-character passwords (letters digits and symbols that are never stored digitally).

When staff work away from the office (usually at home), they do so through a Virtual Private Network or VPN. This provides a secure launching pad, again password protected, before access to the server is made via the web.

When we archive information from the server, we move it onto a backup hard drive. The hard drive is locked away in the office.

3. Communications.

Information is often exchanged internally and externally by email. We use Office 365 which is a cloud based solution provided by Microsoft please see https://technet.microsoft.com/en-us/library/dn532171.aspx providing detail on security and compliance. Each staff member saves the emails in their account online and periodically moves pertinent client detail over to the database. Once the key points are transferred to the database, emails need to be deleted within a few months of the end of the case/correspondence

4. Payment Card Industry Data Security Standard (PCI DSS) Compliance

We ensure we comply to the Data Security Standards and that your personal card information is secure as follows:

Use of the technology

- Members of the fundraising team are authorised to take payments over the phone, through the Sage Pay terminal. Authorised staff request:
  - the name and phone number of the buyer/donor
  - the 16-digit number, expiry date and the 3 card verification security numbers on the back of the card.
  - No PIN numbers are requested or taken.
- Staff must enter these details on Sage Pay directly while the donor is reading out the details. They are NOT allowed to make a note of the details in any other way.

- Only these authorised staff may process email orders with debit card information.
- Under no circumstances may account/card information be requested or sent via end-user messaging technologies i.e. via e-mail, messenger, text or any other form of electronic media.

- A record of the purchaser/donor's name and phone number is kept on the Raiser's Edge database along with the amount paid.
- There are no other internal or external distribution of any paper or electronic media containing cardholder information. No data may be shared with other service providers.

Security Incident
If a security incident comes to the attention of any staff member, they must immediately report to one of the managers who will investigate immediately, inform the Executive and contact the police and other relevant authorities. Disciplinary procedures will be instigated as appropriate.

Security Awareness Programme and Policy Audit
The Fundraising Manager undertakes an annual risk assessment and review that covers this area of practice, reports on our compliance as required to Barclays and reminds all staff of this policy.

5. Mobile phones.

The charity has provided 6 mobile phones for staff to use. 3 are with our Outreach workers who work from home and the other 3 are for office-based staff. Each phone can access the database, access the Office 365 email, social media and use texting as a means of business communication. The phones provided are factory encrypted and password protected with a PIN. Staff are advised not to leave them unattended at any time and to extend their PIN from a 4-digit code to a 6 digit code. Phones can be remotely wiped in the event of theft. Texts should be wiped every month.

6. Facebook account enquiries

Please see guidance provided by Facebook on email communication . Whilst on occasion families and individuals message us openly on Facebook to make an enquiry for support, our policy is to

offer support privately away from Facebook. This is done via the private messaging facility initially within Facebook and then via our own email system.

7. Hard copies of information

Very occasionally these are needed by staff at home or when making visits and must be kept as securely as possible. Staff minimise their carrying of personal information

8. Handwritten notes

These are gathered from phone calls or visits that are later referred to and transferred to Raisers Edge and must be placed in a secure place at the end of the day. If notes need to be transported by staff, they must be kept securely. Once copied any notes must be confidentially shredded.

9. Day to day care

Staff must never leave personal information: unattended in a vehicle; out on their desks or in their home where people other than SMA UK staff may see them. This includes never leaving an unattended computer screen with personal information visible.

10. **Finance and staff personnel records**.

Prior year and active year financial records are kept on site and locked in a steel cupboard. 6 years of older financial records are kept in a locked secure room. Previous staff personnel records are kept locked in a steel cabinet as are active personnel and trustee records. All onsite records are locked within an alarmed building. Access to these electronic folders is restricted to managers.

11. **In the event of a breach.**

Whilst the risk of a “category one cyber attack” is improbable for us, the most likely threat comes from information being sent to the wrong people or a member of staff losing or having an unencrypted device stolen or a fraudulent attack via the website. Under the changes to the GDPR it is now mandatory to inform the ICO within 72 hours of any personal data breach which affects people’s “rights and freedoms”. Businesses will also have to inform data subjects “without undue delay” if there is a “high risk” to those rights and freedoms.

a. We will treat all sources of reports as a potential security incident unless we have indications to the contrary.
b. We will complete a notification and risk analysis See **Appendix 12**
c. We will investigate the nature of the information disclosed, to whom it affects and the likely consequences to the individuals.
d. We will take steps to address the breach or minimise the impact of the breach on the data subjects. This will be done in timely manner. Steps may include; a system lock down, account lock down, notifying banks or credit card companies.
e. We will openly and honestly communicate with the ICO, the press, social media and data subjects throughout the process.