DATA PROTECTION FOR VOLUNTEERS
Update & Summary Guidance February 2026

Data Protection Policy – key points

- Under Data Protection legislation, Cranfield Trust is the **'data controller'** so we need to know what **'personal data'** is being held and processed by volunteers. We have a responsibility for protecting the data and to make sure it is only being used for our declared 'lawful purposes'

- **'Personal data'** is anything that identifies an individual living person, even if it doesn't include their name. It could be an email address, a photograph, some notes or other characteristics that when combined might help to identify them. We are particularly concerned with protecting personal data.

- We now ask all our client charities to sign a **Data Sharing Agreement** which sets out the responsibilities of the client and the Trust. You can view this by visiting the privacy page on our website. We also ask all our volunteers to undertake to avoid processing data that identifies individuals, eg by removing identifiable characteristics ('anonymising') when making notes recording the substance of advice or guidance provided to the charity

- There are some common-sense things everyone can do to keep data safe, such as not sharing it with unauthorised people, protecting it when it is transmitted or stored and handling it responsibly. For more details, refer to Section 5 of the detailed policy.

- After your assignment has finished, we've updated our guidance on what you should do with any personal data you hold:
  - You may retain documentation for up to 3 months to allow for circumstances where ongoing contact or further queries arise from the client charity. In some cases (eg a mentoring relationship), there may be a requirement to maintain data for a much longer period but you should notify the Trust if this is necessary.
  - In some areas of 'regulated' advice or guidance (such as insolvency advice), there may be a need to retain details of the substance of advice provided. In these circumstances you should endeavour to record an anonymised summary of the advice provided which retains enough pertinent information to allow for further queries to be answered.
  - After a reasonable retention period, and subject to the preparation of 'summary notes', any further documents or files that identify individuals should then be deleted from your systems or destroyed by secure means (ie not using general household waste or recycling).
  - If you are concerned that more substantial details need to be retained then these should be forwarded using secure means to the appropriate staff at the Trust for uploading to the secure CRM system. The links to resources and further reading below signpost you to guidance on bulk sending of emails and attachments using compression methods.
  - The Trust's policy is to retain relevant data for up to 6 years. If you hold Personal Data on historical assignments going back further, you should undertake to delete your records as soon as possible (subject to the provisions above).
  - In some circumstances, you may wish to retain contact with the charity in your personal capacity beyond the engagement under the auspices of the Trust. In this situation, you would become a Data Controller in your own capacity, and you should seek the consent of the individual Data Subjects (eg a contact at the client charity) before processing or retaining their data.

- We have recently updated our general guidance ('Dos and Don'ts'), including an update to guidance on using cloud storage providers for backup, and adopting 'Multi Factor Authentication' methods for providing secure access to systems. Please refer to Section 9 of the detailed policy.

DATA PROTECTION FOR VOLUNTEERS
Update & Summary Guidance February 2026

- In a 'Post-COVID' world, we accept that the majority of our interactions (eg between volunteer and client charity are now 'remote' rather than face to face. We provide guidance on what sort of things to think about when connecting online, for example safeguarding a charity's beneficiaries and respecting confidentiality. You can find more in Section 11 of the detailed policy.

- We have now introduced some guidance around the use of Artificial Intelligence (AI) technologies which may impact our work with charities, and some details of the risks and data protection areas to consider when using AI tools. You can read more about this in Section 10 of the detailed policy.

- If you think data has been compromised or lost, you must report it straight away to your primary contact (eg Project Manager) at the Trust, who will then report to their colleague who will record and investigate an 'incident' as necessary. More guidance can be found in Section 12 of the detailed policy.

- We now ask all our volunteers when they register to indicate that they have read and agree to abide by the terms of the Data Protection Policy.

- We provide additional guidance on our Volunteer Hub that you might find useful, such as:
  - **Frequently Asked Questions (FAQ)** which includes more detailed examples of particular areas such as cloud storage, virtual private networks, data subject access requests and so on.
  - A **'how to' guide** on compressing lots of emails and attachments into a single file which can be emailed back to the Trust (should you ever need to do this). This may be useful if you think there is a need to retain detailed (and often complex) 'threads' relating to individual assignments.

- We are always looking into ways that technology can make things easier for our volunteers. For example, whilst it is impractical and not cost-effective to provide a Cranfield Trust 'mailbox' for all of our volunteers, a future aspiration is to allow our volunteers to provide 'progress reports' which will update details in our 'CRM' system. Last year we set out a wider technology strategy for Cranfield Trust, and this kind of system access will be one area we will consult our technology partners about. We will keep you posted as things develop.