	c:\users\admin\onedrive - the cranfield trust\communications, marketing and insight\marketing\branding\templates\dp policy - volunteers final v9 rebranded.docx				
	Date Created	19/10/2020	Author:	James Lennard	
	Version No.	Last Review	Approved By	Approved On	Next Review
	9	09/03/2022	CT Board	13/10/2022	12/10/2023

Data Protection Policy - Volunteers

1. Purpose and Scope

This policy is designed to enable volunteers of Cranfield Trust (the “Trust”) to comply with the law and follow good practice in respect of the data they may hold or process about individuals in relation to the Trust’s activities with charity clients and their staff, volunteers and workers as well as other confidential information.

This policy applies to “**Personal Data**” and “**Confidential Data**”.

“**Personal Data**” is “any information relating to an identified or identifiable natural person” (the “**Data Subject**”) as defined by the General Data Protection Regulation 2016/679 (“GDPR”) and for the purposes of the UK Data Protection Act 2018 (together, “**Data Protection Law**”). The Trust is a **Data Controller** for the purposes of Data Protection Law in relation to Personal Data.


“**Confidential Data**” can include data which does not identify individuals, but which may identify an organisation, or is of a sensitive or confidential nature to the charity client or business with which the Trust conducts its activities. This may include business plans, proposals, financial information, forms, diagrams or templates.

We expect any staff or volunteers acting under the auspices of the Trust to abide by the Trust’s policies and processes in relation to both Personal Data and Confidential Data.

2. Data Sharing / Non-Disclosure Agreements

Both the client charity and the Trust are Data Controllers for the purposes of Data Protection Law in relation to Personal Data. This means that the client charity has a responsibility for notifying (and in some cases gaining consent from) its Data Subjects before sharing Personal Data with the Trust. The Terms relating to data sharing between the Trust and the client charity are set out in the [Data Sharing Agreement](#).

The client charity may wish to enter into a Non-Disclosure (NDA) or Confidentiality Agreement with the Trust in relation to the activity, and in most cases this will cover the support provided to the client charity by the Trust’s volunteer or staff member, since the client charity ‘contracts’ directly with the Trust. In some cases, the client charity may insist on the volunteer signing an NDA with the client charity directly. The Trust is able to provide a template NDA if required. If you have any questions about this, please contact the Trust’s Head of Finance, Administration and Control (details below).

	c:\users\admin\onedrive - the cranfield trust\communications, marketing and insight\marketing\branding\templates\dp policy - volunteers final v9 rebranded.docx				
	Date Created	19/10/2020	Author:	James Lennard	
	Version No.	Last Review	Approved By	Approved On	Next Review
	9	09/03/2022	CT Board	13/10/2022	12/10/2023

Data Protection Policy - Volunteers

3. Lawful Purposes


The lawful purposes for which the Trust collects, holds and processes Personal Data are set out in the Trust's [privacy notices](#).

The Trust's Legitimacy Impact Statement sets out the key legal bases for processing of Personal Data in relation to different types of stakeholder. If you would like a copy of this document, please email us at mydata@cranfieldtrust.org.

4. Principles of Data Protection

The Trust has a responsibility to comply with the requirements of Data Protection Law which sets out the following **seven principles of data protection**:

1. **Lawfulness, fairness and transparency** – Personal Data must be processed lawfully, fairly and in a transparent manner;
2. **Purpose limitation** – Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. **Data minimisation** – Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Wherever possible your activities for the Trust should be carried out without the recording of Personal Data;
4. **Accuracy** – Personal Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. **Storage limitation** – Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

	c:\users\admin\onedrive - the cranfield trust\communications, marketing and insight\marketing\branding\templates\dp policy - volunteers final v9 rebranded.docx				
	Date Created	19/10/2020	Author:	James Lennard	
	Version No.	Last Review	Approved By	Approved On	Next Review
	9	09/03/2022	CT Board	13/10/2022	12/10/2023

Data Protection Policy - Volunteers

6. **Integrity and confidentiality (security)** – Personal Data must be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;
7. **Accountability** – the Trust is responsible for, and must be able to demonstrate compliance with Data Protection Law.

5. Key Responsibilities

The Trust’s Board of Trustees has overall responsibility for ensuring that the Trust sets policies that comply with its legal obligations as the Data Controller. The setting and review of policies, including Data Protection, is delegated to the Audit and Risk Committee (ARC). Day to day responsibility for data protection rests with the Head of Finance, Administration and Control (Head of FAC).


We expect all our volunteers to abide by any policies and procedures that relate to Personal Data they may handle in the course of their activities. In practice this will mean that at all stages, Personal Data is:

- handled responsibly
- never left unattended in areas accessible by members of the public
- never shared with stakeholders without appropriate permissions
- kept up to date as far as possible
- adequately protected when in transit
- securely stored at a private residence or office
- not duplicated or shared unless absolutely necessary
- not retained for longer than necessary, and deleted or returned at the end of an assignment

6. Code of Conduct

Volunteers should act in the best interests of the Trust at all times. As representatives of the Trust, volunteers are required to adhere to the following general principles:

- **Confidentiality** – personal details of individuals, confidential business relationships, activities and other confidential matters should not be disclosed to other clients, third parties, staff or volunteers without appropriate permissions (see below). Volunteers should abide by this principle in all environments in which they operate in

	c:\users\admin\onedrive - the cranfield trust\communications, marketing and insight\marketing\branding\templates\dp policy - volunteers final v9 rebranded.docx				
	Date Created	19/10/2020	Author:	James Lennard	
	Version No.	Last Review	Approved By	Approved On	Next Review
	9	09/03/2022	CT Board	13/10/2022	12/10/2023


Data Protection Policy - Volunteers

connection with their works associated with the Trust, including relationships formed through social networking and similar media. This also applies to data held in any format, including on personal mobile communications devices.

- **Integrity** – volunteers should be aware that they represent the Trust in all forms of business communication, be it with the Trust’s colleagues, clients or other contacts. As such, everyone should seek to communicate in a clear, professional and courteous manner.
- **Professionalism** – volunteers must make every effort to separate private opinions from the professional opinions of the Trust, and to make it clear that a personal opinion is being expressed, rather than a formal opinion of the Trust. For example, this could come about when referring to the Trust’s activities using a private social media account such as Twitter

All conduct should be in accordance with this policy and the requirements of Data Protection Law and Privacy and Electronic Communications Regulations (EC Directive) (2003) (PECR) in respect of the handling of personal information.

As a general rule, all staff members of the Trust have appropriate access to personal data via the Trust’s systems, and appropriate clearance in processing personal data, but it should be presumed that clients, volunteers or third parties do not. If in doubt, check with your primary contact at the Trust or with the Head of Finance, Administration and Control (details below).

	c:\users\admin\onedrive - the cranfield trust\communications, marketing and insight\marketing\branding\templates\dp policy - volunteers final v9 rebranded.docx			
	Date Created	19/10/2020	Author:	James Lennard
	Version No.	Last Review	Approved By	Approved On
	9	09/03/2022	CT Board	13/10/2022
			Next Review	12/10/2023

Data Protection Policy - Volunteers


7. What forms of data are we concerned with?

The following types of data are representative of the data that may be held or processed by volunteers in the course of their activities for the Trust:

Personal Data	
'Case Notes'	Handwritten or electronic records of telephone conversations which identify individuals in relation to charity clients, ie name of individuals, the charity's name, email addresses, telephone numbers etc.
Email / SMS	Email addresses and names of individual recipients and their association with a charity, ie clearly identifiable within the email addresses used.
Email / SMS continued	Named individuals and their associated data (eg job title, date of birth etc) from the body of an email conversation. Email attachments which may identify individuals as above. Name and telephone number forming part of an SMS conversation.
Documents	Any other documents or correspondence containing data which identifies individuals and their characteristics.
Online information and advice services	Historical 'case notes' from a volunteer's interaction with charity clients which may support a 'question and answer' thread or advice and guidance (eg for HRNet).
Confidential Data	
Documents	Documents such as policies, proposals, forms, templates, diagrams, financial information and other correspondence which do not identify individuals but which may be sensitive or confidential to the charity client to which they relate. Care should also be taken to protect and respect copyright and intellectual property when handling any information provided by the client.

8. What to do with Personal Data


Whatever form of data is processed, the Trust is particularly concerned with protecting data that volunteers process which may identify individuals or reveal sensitive

	c:\users\admin\onedrive - the cranfield trust\communications, marketing and insight\marketing\branding\templates\dp policy - volunteers final v9 rebranded.docx				
	Date Created	19/10/2020	Author:	James Lennard	
	Version No.	Last Review	Approved By	Approved On	Next Review
	9	09/03/2022	CT Board	13/10/2022	12/10/2023

Data Protection Policy - Volunteers

characteristics relating to individuals. The following sets out our expectations around what should happen to Personal Data once an assignment has ended:

- You may retain documentation for up to three months beyond the end of an assignment, 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 (eg contact details) for a much longer period but you should notify the Trust if this is necessary.
- We appreciate that in some areas of 'regulated' advice or guidance (such as HR or insolvency advice), there may be a need to retain details of the substance of advice provided well beyond the end of an assignment. As far as possible, in such circumstances you should endeavour to record an anonymised summary of the advice provided (ie by removing references to identifiable individuals) 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 Trust's FAQ (Data Protection) documents provide more guidance on bulk sending of emails and attachments using compression methods.
- Whilst the Trust's insurers advise that data in relation to advice should be retained for three years after the assignment, the Trust retains 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.


	c:\users\admin\onedrive - the cranfield trust\communications, marketing and insight\marketing\branding\templates\dp policy - volunteers final v9 rebranded.docx				
	Date Created	19/10/2020	Author:	James Lennard	
	Version No.	Last Review	Approved By	Approved On	Next Review
	9	09/03/2022	CT Board	13/10/2022	12/10/2023

Data Protection Policy - Volunteers

9. General Guidance on Data Security


When handling any of the above types of data in the course of your activities with charity clients, you should be aware of your responsibilities under section 4 above, and follow these general 'DOs and DON'Ts':

DO	DON'T
Use Personal Data only for the purpose for which it was communicated to you.	Use Personal Data for any other purpose beyond the support you provide through the Trust.
Limit the amount of Personal Data which you process to the bare minimum. If you can carry out your activities without referring to identified or identifiable individuals, you should do so. Do ask the client charity to anonymise or pseudonymise information wherever possible before sharing with you.	Refer to identified or identifiable individuals unnecessarily.
As far as is reasonably practical, use reputable providers for email or cloud storage. The Trust does not hold insurance cover for cyber threats so we work on a 'reasonable endeavours' basis in asking volunteers to be aware of where their data is held or backed up. Our FAQ (Data Protection) document provides some additional guidance and helpful links in relation to cloud storage.	As far as is reasonably practical, avoid backing up documents containing Personal Data or Confidential Data of the Trust on servers located outside the European Economic Area (EEA).
Use a privately-owned computer or phone and your own storage devices to which other people don't have access.	As far as possible, don't use a shared device or an unprotected network.
Password-protect your systems with a strong password. Consider also adopting	Allow other people (colleagues or family members) access to your systems or

	c:\users\admin\onedrive - the cranfield trust\communications, marketing and insight\marketing\branding\templates\dp policy - volunteers final v9 rebranded.docx			
	Date Created	19/10/2020	Author:	James Lennard
	Version No.		Approved By	Approved On
		Last Review		Next Review
	9	09/03/2022	CT Board	13/10/2022

Data Protection Policy - Volunteers

Multi Factor Authentication (MFA) which is regarded as best practice in reducing cyber risks.	storage containing the Trust's data. Don't share your password.
Keep physical and electronic files secure whilst 'at rest' and 'in transit'. For physical documents, consider locked storage, a locked briefcase or a locked office wherever possible. For electronic files, consider using encrypted storage.	Don't leave files containing Personal Data unattended.
Access files and emails, and hold telephone conversations within a private and secure environment. The FAQ (Data Protection) document provides some additional guidance and helpful links in relation to Virtual Private Networks (VPNs).	As far as possible, don't access files, emails or hold sensitive telephone conversations in public places such as cafes or using public WiFi.
Make sure your system is protected with controls such as anti-virus, anti-malware, anti-spam etc and that these products are kept up to date.	Don't use any system if you are unsure about the adequacy of its controls, eg up-to-date anti-virus, anti-malware software etc.
Securely destroy case notes, files and emails once you have forwarded them to your principal contact at the Trust. Consider the use of a secure shredding device.	Dispose of case notes, files and emails in an unsecure manner.
Keep the details of your interactions and conversations with clients private, in particular where the identity of individuals is concerned.	Share private details of individuals with non- Trust colleagues or family members or with individuals within the Trust who do not have a need to know.
Check that your information is up to date,	Keep hold of contact information, eg email

	c:\users\admin\onedrive - the cranfield trust\communications, marketing and insight\marketing\branding\templates\dp policy - volunteers final v9 rebranded.docx			
	Date Created	19/10/2020	Author:	James Lennard
	Version No.	Last Review	Approved By	Approved On
	9	09/03/2022	CT Board	13/10/2022
			Next Review	12/10/2023

Data Protection Policy - Volunteers

eg the email address of a contact to ensure that the correct recipients are contacted or sent information.	address or phone number for any longer than is necessary. Always check with your Trust contacts if you need up to date contact information.
Always check the recipient's email address before sending, and take care when using 'autocomplete' settings for the 'To' fields in emails, especially when the intended recipient has the same name as another address book contact.	Release an email when you are at all unsure about the recipient's email address, or there is a suspicion that an unauthorised colleague can access the recipient's emails.

10. 'Remote' contact, data protection and safeguarding

Section 8.2.3 of the Trust's Safeguarding Policy contains guidance on data protection, confidentiality and safeguarding considerations when conducting 'remote' (online) meetings with charity clients. You should ensure that you have read this guidance and are aware of some of the potential risks associated with conducting remote meetings, either by videoconference or voice-only calls. For further details, please refer to the [Cranfield Trust Way](#) document.


11. Data Incidents and Breaches

All volunteers who manage or control data have a responsibility under Data Protection Law to ensure appropriate and proportionate security of the Personal Data they hold. Any misuse of data will be fully investigated and could result in the termination of the Trust's relationship with you or legal action if the incident is sufficiently serious.

Information is considered **lost** whenever:

- it cannot be physically produced or its disposal accounted for after reasonable steps have been taken to locate it;
- it is reasonably presumed to have been destroyed by fire, flood or other natural means, by accident.

Information is to be presumed **compromised** whenever:

	c:\users\admin\onedrive - the cranfield trust\communications, marketing and insight\marketing\branding\templates\dp policy - volunteers final v9 rebranded.docx				
	Date Created	19/10/2020	Author:	James Lennard	
	Version No.		Approved By	Approved On	Next Review
	9	09/03/2022	CT Board	13/10/2022	12/10/2023

Data Protection Policy - Volunteers

- an unauthorised person has had access to all or part of the information, for example where confidential information has been put in the waste paper bin rather than confidential waste;
- material is lost in circumstances where an unauthorised person may have access to it, for example where a laptop has been lost in a public area or when a set of keys to locked storage are mislaid


A **breach** of security occurs where information has been put at risk. The list below is not exhaustive but examples include:

- Loss of information.
- Compromise of information.
- Failure to immediately report the loss or compromise of information.
- Unauthorised removal of information from an approved or authorised location.
- Incorrect transmission of information where neither loss nor compromise has occurred.
- Unauthorised or deliberate disclosure of personal or Confidential Data.
- Loss or misplacement of keys or entry codes to locked storage or restricted areas.
- Information missing in the post or from a fax transmission.
- Theft of a computer, laptop or memory stick containing Personal Data
- Loss of a mobile phone containing Personal Data.
- Leaving manual records such as files or a laptop containing personal information on a train or in any non-secure environment.

It is very important that any breach of security is reported without delay in order for remedial action to be taken if necessary and to comply with legal obligations such as data breach notifications under Data Protection Law. In the first instance, a breach of security should be reported immediately to your primary contact (Project Manager) who in turn will report the breach to James Lennard (Head of FAC) to be logged, assessed and investigated.

A security incident notification should include:

- The type of information and number of records
- The circumstances of the loss / release / corruption

	c:\users\admin\onedrive - the cranfield trust\communications, marketing and insight\marketing\branding\templates\dp policy - volunteers final v9 rebranded.docx				
	Date Created	19/10/2020	Author:	James Lennard	
	Version No.		Approved By	Approved On	Next Review
	9	09/03/2022	CT Board	13/10/2022	12/10/2023

Data Protection Policy - Volunteers

- Action taken to minimise / mitigate effect on individuals and whether they have been informed
- Details of how the breach is being investigated
- Whether any other regulatory body or contractor has been informed and their response
- Remedial action taken to prevent future occurrence

The Head of FAC will coordinate an investigation and create a detailed breach incident report and discuss with the Trust’s CEO to mitigate organisation-wide breaches of a similar nature and to instigate any possible solutions for the breach. The incident will be logged in a Breach / Incident Log.

Dependent on the seriousness and circumstances the breach may be reported to the Trust’s Board and then to the Information Commissioner’s Office and in some cases to Data Subjects.


Under no circumstances should any security breach/incident be reported to the Information Commissioners Office or any other third party (i.e. the press) without obtaining prior authority from the Trust.

Declaration – Volunteers Working on Trust Assignments

By accepting this assignment on behalf of the Trust you acknowledge that the Trust is a data controller for the purposes of data protection legislation and in continuing in that function you agree to abide by the terms of the Trust’s Data Protection Policy for volunteers (version 9, dated 09/03/2022).

I have read and understood and will abide by the Trust’s Data Protection Policy for volunteers (version 9, dated 09/03/2022). In particular, I commit to the following:

- I will handle any data which identifies individuals or is of a sensitive or confidential nature with due responsibility and with regard to principles of information and systems security in accordance with this policy;
- I will only use Personal Data for the purpose for which it has been provided to me;
- I will not share or disclose Personal Data or Confidential Data to unauthorised recipients, including telephone conversations of a confidential or sensitive nature;

	c:\users\admin\onedrive - the cranfield trust\communications, marketing and insight\marketing\branding\templates\dp policy - volunteers final v9 rebranded.docx				
	Date Created	19/10/2020	Author:	James Lennard	
	Version No.		Approved By	Approved On	Next Review
	9	09/03/2022	CT Board	13/10/2022	12/10/2023

Data Protection Policy - Volunteers

- Where I or the Trust deem it necessary to retain a summary of advice and guidance provided as part of an assignment, I undertake to record an anonymised summary and forward a copy of this to the Trust, retaining a copy for my own records;
- Where I or the Trust deem that there is a need to retain details of advice and guidance provided as part of an assignment, I undertake to forward all relevant retrospective electronic data (eg 'case notes') and documentation to the Trust's staff for secure processing and retention via the Trust's CRM system; I undertake to forward all relevant data for ongoing assignments in the same manner;
- I have destroyed all copies of such case notes and documentation in relation to prior assignments, and I undertake to confirm in writing that all relevant data will be destroyed at the conclusion of each ongoing assignment;
- I will not keep other Personal Data beyond the relevant retention period, including individual contact details such as email addresses and telephone numbers, without the express consent of the individual concerned;
- I will report any breach of security to my Primary Contact immediately, including where any systems have been compromised or attacked by viruses or malware, or an email has been sent to the wrong recipient;
- I will have due regard for copyright, confidentiality or intellectual property provisions as required by the client and will make my Primary Contact aware of any additional requirements communicated to me by the client;
- I will conduct my activities in a professional manner and I am aware that any deliberate or reckless disregard for guidance issued by the Trust may invalidate the Trust's professional indemnity insurance provisions in relation to volunteer assignments. A severe breach or compromise of data may result in the termination of my engagement with the Trust and the pursuance of legal action against me.

If you have any questions in relation to this policy, please contact James Lennard, Head of Finance, Administration & Control (mydata@cranfieldtrust.org).