FREQUENTLY ASKED QUESTIONS – DATA PROTECTION FOR VOLUNTEERS

What is difference between 'Personal Data' and 'Confidential Data' and should I treat them differently?

'Personal Data' is any data that identifies a living individual (the 'Data Subject'). It could include a person's name, email address, a unique identifier or a combination of pieces of information which when combined, identify the individual. Note that some data may not necessarily identify the individual, eg ethnic origin, gender identification, sexual orientation and medical conditions but if this information fell into the wrong hands, it may provide pointers as to the identity of an individual, so should be treated sensitively. A good rule of thumb is to ask whether, if the data went astray, would it impact the rights and freedoms of an individual person.

'Confidential Data' is data which does not identify an individual, but may be confidential (because of its sensitivity) to the client charity. This could include business plans, proposals, financial information, contracts, forms, charts, diagrams, organizational structures, templates, policies, scenarios and so on. You should still take steps to protect such data, but since it does not identify an individual, it does not fall into the scope of data protection legislation (eg GDPR).

My contact at the client charity uses a work email address, eg joe.bloggs@charity.org.uk. Does this still identify them as an individual, even though it's not a private email address?

Your contact's email address may not on its own identify them as an individual, especially if they have a common name. However, it is always worth reflecting on whether this information, combined with other forms of data (eg phone number, business address, the charity's website) could help someone to identify them in their private capacity. For example, from the email address, it could be possible to track them down via the charity's website, obtain a photograph, locate them via social media or other records in the public domain, and eventually form a full picture of the individual which could be exploited for nefarious means, affecting the rights and freedoms of that data subject.

What sort of things should I be aware of when considering data security in relation to my assignment?

There are a few basic steps you can take to make sure your interactions with the charity, and any data that you process, is kept secure. Below is a summary of the sorts of things you should consider, and for more information, please refer to the 'Do and Don't' section (pages 7-9) of the Trust's Data Protection Policy for volunteers.

- Keep the amount of personal data you use to a bare minimum, and consider 'anonymising' any references to individual data subjects in your case notes etc
- As far as possible, only use devices that are not shared with others
- Access data or hold conversations in relation to your assignment in a private, secure environment wherever possible
- Password protect your systems with a strong password
- Make sure your devices are protected with the latest controls, eg anti-virus, anti-malware, anti-spam and so on
- Check that any personal information you hold is up to date, and that you are corresponding with charity contacts using the correct addresses. Take care when using 'autocomplete' fields in emails, for example

- Take secure backups of your data using recognised providers or systems
- Only keep the absolute minimum levels of information required for you to carry out the assignment
- Have regard to 'safeguarding' whenever you have contact with the charity via videoconferencing facilities. Safeguarding can apply to the charity's service users but also your own family members

I'm seeing a lot about 'AI' technologies and their use in the workplace. What sort of things should I be aware of in relation to AI that might impact my assignments?

We've now included some guidance on AI and the sort of things to be aware of in Section 10 (starting on page 9) of our updated policy. This gives some pointers in relation to 'data subjects', their consents, the processing and security of data. It is important that AI does not encompass one particular process, tool or application but can touch upon many areas of our work, including telephone calls, emails, video meetings or the processing or storage of data.

What makes for a 'strong' password?

There are a number of elements to consider when creating a strong password for your systems. It is best practice to avoid anything obvious like your name, key dates or reference numbers within a password, or even words like 'password'! Combinations of alphanumeric, numerical, upper and lower case letters and symbols are generally regarded as more secure, as well as the number of characters you use – passwords with more than 16 characters are much harder to 'crack' than those with fewer characters. Best practice is to consider constructing your password from a phrase or unrelated combination of words rather than a random collection of numbers and symbols, eg HOW!n0w!Brown*COW

There are a number of 'password manager' apps available which help you to manage and generate passwords for your various systems and accounts. There is also an increasing move towards 'multi-factor authentication (MFA)' for well-known systems, whereby other 'tokens' are used in conjunction with username and passwords, such as QR codes, text or email codes.

My charity sends me 'hard copy' documents to work with as part of the assignment, or I have to print off copies to work with. Are there any particular security considerations I should be aware of?

If the 'manual' files contain personal data, then a good rule of thumb is to think about security of those documents when 'in transit' between you and the charity, and when 'at rest', ie in your possession. Since the information may belong to the charity, they should take responsibility for ensuring that documents reach you in a secure manner, eg by using 'tracked' mail or courier options, and by ensuring that the documents are securely packaged. If you need to send hard copy documents back to the charity, or indeed to the Trust for safe storage, then you should follow the same process.

When working with hard copy files containing personal data, you should as far as possible only access those files in a private and secure environment such as a home office. When not in use, consider locked storage such as a locked room, drawer, filing cabinet or briefcase. If you need to move the files between locations, for example between home and an office, you should keep them secure in a locked briefcase for example.

The charity I am working with has said they will send me confidential data in relation to my assignment. This data identifies individuals. What should I do to make sure this data is kept secure?

The first thing you should do is question whether it is absolutely necessary for the assignment that you have sight of this data – in most cases you shouldn't need to see individuals identified, even though you could see financial data. Ask the charity to 'anonymise' the data before they send it to you.

If they do decide that it is absolutely necessary to send you this data, then first and foremost the charity needs to be made aware that they are the controller of their data for the purposes of data protection legislation (this is covered by the 'Data Sharing Agreement' between the charity and Cranfield Trust). For example, the charity must make sure that it has the permission of the 'Data Subject' (the individual) before they share data with you. Since they take the risk if data is sent outside their organisation, the charity should make sure the data is sent to you in a secure manner, eg by encrypted email or encrypted cloud storage. At the end of the assignment, you should ask the charity whether they want this data destroyed or returned to them.

My charity has asked me to sign a Non-Disclosure Agreement (NDA) in relation to the assignment. Should I sign this?

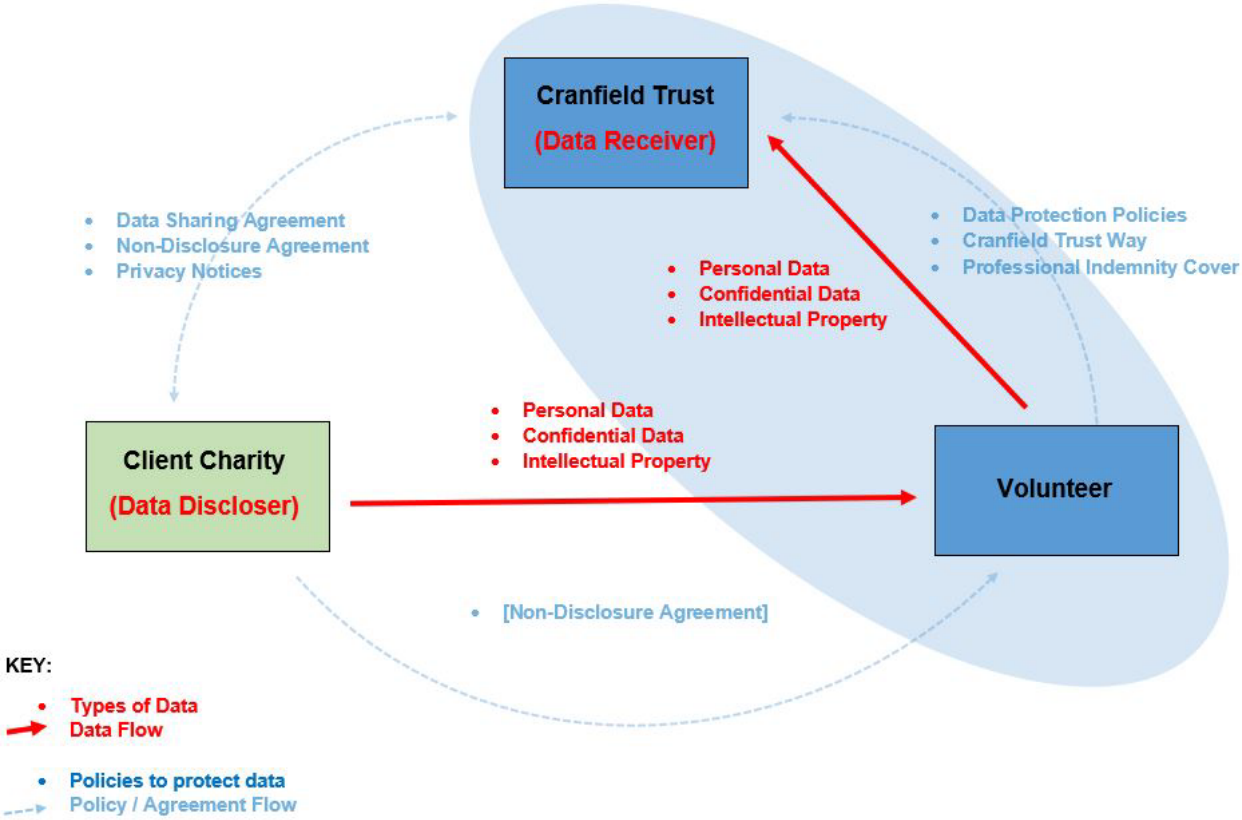
Strictly speaking the assignment is between the charity and Cranfield Trust, and you act as an agent of the Trust. The Trust's Data Sharing Agreement covers the responsibilities of the charity ('Data Discloser') and the Trust ('Data Receiver') and describes the flow of data and how it is protected during and after the assignment. If a charity asks for an NDA o be signed, you should first direct them to the Trust who will ask to be a party to the agreement, and can propose a template NDA. If the charity absolutely insists that you sign an NDA in your personal capacity, you can do so but you should be aware that in this event, if there is any breach of confidentiality, the charity may hold you personally liable under the terms of the NDA. The Trust would generally want to avoid putting additional risk or responsibility on its volunteers in this way. If in any doubt, please contact the Trust (details below) and we can advise you.

I'm a bit confused about the responsibilities of the charity, myself and Cranfield Trust in relation to data that passes between the parties as part of my assignment. Can you explain more about the 'data flow' and who takes responsibility for protecting information?

The Trust's Data Sharing Agreement sets out the responsibilities of the charity and the Trust in relation to data which passes as part of your assignment. For the purposes of data protection legislation and professional indemnity insurance, you work under the auspices of the Trust – the charity does not engage you directly in your private capacity.

Please see the following extract from the Data Sharing Agreement which illustrates the 'data flow' and respective responsibilities of the various parties:

Flow of Data in relation to Management Consultancy and other assignments



What should I do with 'case notes' and other documents beyond the end of my assignment?

Since the assignment was provided by you under the auspices of Cranfield Trust, you should forward key documents (containing the substance of the advice /guidance provided to the charity) to the Trust for secure retention within their systems. The Trust has professional indemnity cover which protects you and its staff, should a charity bring a claim of malpractice against the Trust, so it is imperative that the Trust is able retain reasonable notes on the substance of the assignment in order to defend a potential claim. This requirement needs to go back up to 6 years from the end of the assignment.

The Trust is also the 'data controller' under data protection legislation, and so needs to demonstrate that it has measures in place to protect personal data which is processed as part of the assignment. If any of your documentation contains personal data, you should forward it to the Trust at the end of your assignment and you should destroy any information containing personal data. The Trust will securely retain documents in accordance with its data retention policy.

I wish to maintain contact with the charity in my private capacity beyond the assignment. Is this acceptable?

Continued contact with the client charity is often requested by both parties when a productive relationship has developed through the assignment. You can maintain contact with the charity in your private capacity but you should be aware that you would become a 'data controller' in your own

capacity, processing the personal data of your contacts, who are 'data subjects'. It is good practice to seek the charity's consent for you to retain contact details and other information.

Can I still retain important documents in relation to the assignment if the 'personal data' has been removed?

As far as possible, you should seek to limit the amount of data relating to individuals in any information you have access to or need to use in relation to your assignment. If you need to retain case notes, plans etc which provide a substance of the advice given beyond the end of your assignment, you may do so but you must ensure that any references to data subjects are removed from the information in your possession. This could include, names, addresses, email addresses or telephone numbers. You should also consider things like job titles, roles or other references within your 'case notes' that may identify the individual.

What does 'anonymisation' and 'pseudonymisation' mean?

'Anonymisation' is the removal of identifiers of individual data subjects from information, for example replacing someone' name with 'Person X'.

'Pseudonymisation' is the replacement of an identifier for an individual data subject with another unique indentifier (eg a code number) which in on its own will not identify the individual, but when cross-referenced with another data set, could identify them. An example might be a list of payroll data with 'Payroll Number' used as the identifier of an individual, rather than their name.

Anonymised data is not regarded as personal data by GDPR, whereas Pseudonymised data may come under the legislation.

My charity wants me to attend online 'videoconferencing' meetings from my home with contacts at the charity's offices or other remote locations. Is this acceptable?

The Trust's safeguarding policy contains guidance on what to consider when conducting 'virtual' meetings with charity contacts. It is not a problem for you to attend these meetings as part of the assignment but you should consider confidentiality, data protection and safeguarding if such contact is required. For example, think about the following points:

- Are vulnerable beneficiaries or staff/volunteers observable through a 'webcam', including any background photos? Attendees may wish to consider blurring their webcam background or substituting a safe image if the technology allows
- Is it possible to verify the identity of 'remote' meeting attendees? It may not be enough to use voice-only communications if there are concerns about the sensitivity of a conversation
- Is confidential information viewable through a webcam, eg folders in the background displaying the names of staff or beneficiaries? Attendees may wish to consider blurring their webcam background or substituting a safe image if the technology allows

Use a headset / microphone wherever possible, especially if confidential matters are to be discussed. Many online meetings may take place in at least one attendee's home and often family members or other occupants could be in the background, or photos of children.

I use a 'webmail' and 'cloud storage' provider to back up my documents etc. What should I be aware of in relation to data security?

Whilst it is not always easy, you should ideally check to see where your data is held and backed up. Recognised storage providers (eg Microsoft, Amazon, Google, Dropbox etc) may store the data across multiple data centres and in multiple country locations so as a minimum it is worth checking on whether data is stored in the European Economic Area (EEA) or the UK since data protection laws outside of those areas may not be relied upon if your data goes missing. Storage on servers outside the EEA or UK is known as 'offshoring' and some charities, for example with UK government contracts, may be dissuaded from offshoring their data so it is worth double-checking with your client charity whether their own policy applies such restrictions.

It is also worth enquiring about how storage providers keep your data secure, how it is encrypted, and how long they retain it for after you delete your files.

Here are some useful links to general guidance around cloud security:

https://www.ontrack.com/en-gb/blog/where-on-earth-is-cloud-data-actually-stored

https://www.trustradius.com/cloud-storage

https://www.bu.edu/tech/support/information-security/security-for-everyone/how-to-safely-store-your-data-in-the-cloud/

https://us.norton.com/internetsecurity-privacy-cloud-data-security.html

I've heard that it is good practice to use a 'mobile VPN' when accessing data in public areas, eg a café's wifi network. What is a 'VPN' and what products do you recommend?

There are many products for mobile devices produced by recognised security providers (eg Norton) that provide additional layers of protection via a 'Virtual Private Network' (VPN). Essentially this adds an additional secure layer to any communications between your device and a wifi network so that data can't easily be intercepted by other devices on the same network, eg in a public place. It is worth exploring VPN products for your mobile device if you are going to make regular use of public networks.

Here are some useful links:

https://www.ncsc.gov.uk/collection/mobile-device-guidance/virtual-private-networks

https://www.ncsc.gov.uk/guidance/securing-your-devices

https://www.techradar.com/uk/vpn/best-mobile-vpn

A charity has asked for my cooperation with a 'Data Subject Access Request' in relation to the assignment. What should I do in this situation?

First and foremost, if the charity shared any personal data with you as part of the assignment, they should only have done so with the permission of the data subject (ie any individual discussed as part of the assignment). If they did not seek the consent of the individual when sharing data with you, the they could be liable for an action from the data subject under GDPR.
Assuming the charity did gain the consent of the data subject before sharing personal data, then the Trust has a responsibility to cooperate with the charity in the event of a Data Subject Access Request (DSAR). You should have forwarded data to the Trust at the end of the assignment and destroyed personal data that you held. The charity should therefore be put in direct contact with the Trust (details below) to discuss how it can help prepare information in relation to the DSAR.

What data does the Trust hold on me and whose responsibility is it for making sure this is kept up to date?
The Trust maintains contact details for you (such as your name, physical addresses, email addresses and phone numbers) and the names of your referees submitted as part of your application process with Trust. It will then maintain details of your assignments (both accepted and declined) and records of any subsequent contact with the Trust, eg via your regional manager.
Since the Trust has a responsibility under data protection legislation for keeping its information up to date, it is important that you stay in regular contact with the Trust and let staff know if any of your contact details have changed. The Trust can't offer you assignments if it is not confident that it holds accurate contact details.

I have inadvertently sent some sensitive data to the wrong recipient. What should I do?
Section 12 (starting on page 11) of the Trust's Data Protection Policy for volunteers sets out the procedure to follow in the event of a suspected data 'breach'. If you are sure that the data has been sent to the wrong recipient, then it must be presumed that the information may have been compromised, and there is a responsibility to make the data subject (via the client charity) aware of this.
The first step is to notify your primary contact at the Trust (eg your regional manager), providing as much detail of the incident as possible, so that an internal case can be raised. The Trust will treat the incident using a risk-based approach and will take action based on its assessment of the risks to the rights and freedoms of the individual data subject. In extreme cases, the Information Commissioner's Office (ICO) may need to be notified of the breach.

I have mislaid some hard copy files containing personal data. What should I do?
Section 12 (starting on page 11) of the Trust's Data Protection Policy for volunteers sets out the procedure to follow in the event of a suspected data 'breach'. It may be that the information is not lost, but nevertheless you should assume that there is a risk that it has been compromised in some way. There may therefore be a responsibility to make the data subject (via the client charity) aware of this.
The first step is to notify your primary contact at the Trust (eg your regional manager), providing as much detail of the incident as possible, so that an internal case can be raised. The Trust will treat the

incident using a risk-based approach and will take action based on its assessment of the risks to the rights and freedoms of the individual data subject. In extreme cases, the Information Commissioner's Office (ICO) may need to be notified of the breach.

I have lost some personal data that was in my possession. Will I be held liable for this?

In general, you should assume that if you have acted reasonably and have abided by the guidance contained in the Trust's Data Protection Policy for volunteers, then the Trust will take responsibility for the loss of data and will act accordingly in investigating the breach and notifying the relevant parties.

However, the Trust's volunteers are only covered by professional indemnity insurance if they have acted in good faith and not negligently in discharging their responsibilities as part of the assignment. If it is found that you have acted recklessly or with deliberate negligence in relation to keeping information secure, it is possible that the Trust could not rely on its insurance in defending a claim of malpractice brought by either the client charity or the individual data subject. In such an extreme case, it is possible that you would be held personally liable for the breach.