# Volunteer Cornwall
# Secure Transfer and Receipt of Personal and Sensitive Information Procedures

This document outlines the principles and procedures that should be followed where sensitive or personal identifiable information is being transferred to or from systems controlled formally by Volunteer Cornwall. There is a widely acknowledged duty to share information and it is important that where it is proper to do so staff, and volunteers, have the confidence to appropriately share information in the interests of Volunteer Cornwall's work.

These procedures are in place to help prevent unauthorised or unjustified access to information, loss of information, unauthorised disclosure of information or breach of legislation. These procedures apply to all staff and volunteers working in Volunteer Cornwall.

Staff and Volunteers should adopt a wide interpretation of what constitutes a 'transfer' of information. Whenever data becomes accessible outside of the controls implemented by Volunteer Cornwall it can be thought to have been transferred. There are transfers which are self evident, such as the sharing of client information with a volunteer or partner organisation, however there are others which may not be immediately obvious, such as the use of personal devices to access Volunteer Cornwall's remote desktop to work at home, or the inadvertent grant of access to outsiders such as by leaving a visible monitor unlocked when a visitor is in the office.

## Maintaining Confidentiality of Data Received

The Accounts and Administration and Transport Departments are secure physical locations or have the agreed set of administrative arrangements in place within Volunteer Cornwall to ensure confidential personal information is received safely and securely and is passed to the appropriate person without delay. They are also the most consistently staffed departments throughout office hours and so any information received through these teams is less likely to be left unattended prior to being passed to the appropriate individual.

These are the locations for client information to be securely received. All post for Volunteer Cornwall should be opened in the Accounts and Admin department.

## Material received in hard copy

- When paper-based information is received it should be stored securely, as soon as practical, for example:

  (i) Information moved from Accounts and Admin to the secure Transport or Project areas
  (ii) Manual client records should be locked in the filing cabinets when not in use

## Security of IT to prevent inadvertent transfer of data

- Computers should not be left on view or accessible to unauthorised staff:
  (i) Be careful where you locate your computer screen: ensure that it cannot be accidentally or deliberately seen by visitors or staff who do not have authorised access. Be especially careful with computer screens visible from "public" areas of the office, or windows.
  (ii) Always keep your password confidential and do not write it down. Do not share passwords.
  (iii) Password protected screensavers should be used where possible. This is most effectively done using the 'windows' + 'L' keys pressed simultaneously.
  (iv) Laptop computers should be locked up when not in use.
  (v) Where temporary staff, visitors or volunteers are granted use of Volunteer Cornwall IT they

should be provided with their own log-in details and their access set according to the requirements of their anticipated work. The use of generic logins for groups of temporary users should be avoided.

### Other Principles

- Ensure that all waste containing client-identifiable information is cross shredded before disposal or placed for secure disposal.

- Ensure that confidential conversations are held where they cannot be overhead by members of the public. Ensure that sensitive client issues are only discussed in the private areas.

### Only Transfer Data Where Appropriate

The personal information transferred should be limited to the minimum detail necessary for the intended recipient to carry out their role or task required of them.

Before transferring data, consider whether there are any client consent requirements that must be met before the transfer is made:

- A record of consent should be maintained where required.
- A client has the right to choose whether to agree to the use or disclosure of their personal information and the client has the right to change their decision about a disclosure before it is made.
- If circumstances change, relevant to the sharing of consent, for example if there is a change of recipient, consent should be reaffirmed.
- There may be occasions, and situations where it we might treat consent to share information as being impliedly granted and where a formalised consent procedure may act to prevent work being undertaken. For example, where a member of the public is booking transport, it may be fairly inferred that they are happy for the information pertaining to their name and address to be shared with the volunteer driver. However, whenever it is believed that consent to share information is impliedly given efforts should still be made to explain the need to share information, to direct the service user to relevant information online where possible and to obtain their consent to share information.

### Securely Transferring Data

The best method of transferring data will depend a great deal on the context. For example, a less secure method may be more justifiable where time is a significant factor than it would be in less pressing circumstances, and it will rarely be appropriate to share very sensitive information in a less than wholly secure format.

All staff who transfer data should think carefully about the method which they select. The following are relevant considerations in this decision.

- The sensitivity of the information to be transferred.
- The urgency of the need to share the information.
- The known operating procedures of the intended recipients
- The reason for sending the information.

Staff **must not** base their choice of communication on what is convenient for them.

Staff should also consider whether any specific controls are required to maintain the confidentiality of the data e.g., encryption on electronic transfers, or the use of ‘read receipts’.

It is helpful, when deciding on the most appropriate method of transferring information and on what safeguards to use, to carry out a mental ‘Information Risk Assessment’ in which you consider how the

information is likely to be received and what that means for the risks of using that form of communication. Anything which leads to an enduring form of the information is inherently risky, as is anything which receives the information into an insecure context such as a fax machine, rather than a computer with password protection.

Whenever information is transferred, however carefully, there is a risk of either interception, or of the recipient taking less care of that information than we would like. For this reason all staff should exercise some discretion in only transferring the minimum information necessary for the purpose served by sharing the information to be achieved.

## A. Verbal Communication

- Be careful about leaving confidential information in messages on answer-phones. Messages may not be picked up by the intended recipient or may not be deleted.
- Be careful when taking messages off answer-phones. Ensure that the messages cannot be overheard inappropriately when being played back, including by listening to them on a loud speaker when colleagues are themselves on the phone.
- When receiving calls requesting personal information: a) verify the identity of the caller, for example, where this is not a known contact, this can be done by taking the relevant phone number, double checking that it is the correct number for that individual / organisation and then calling the recipient back b) ask for the reason for the request, c) if in doubt about whether the information can be disclosed, tell the caller you will call them back, and then consult with your manager. If you are in any doubt as to the caller's identity, use publicly listed numbers for an organisation to verify that the person requesting the information does work where they say they do.
- Where information is transferred by phone, or face to face, care should be taken to ensure that personal details are not overheard by other people, including staff who do not have a "need to know". Where possible, such discussions should take place in private locations and not in public areas, for example staff room.
- Messages containing confidential / sensitive information should not be left on notice boards that could be accessed by non-authorised staff.

## B. Post

- Ensure envelopes are marked "Private & Confidential"
- Double check the full postal address of the recipient.
- Carefully consider the method for sending confidential information based on risk posed by the loss of the information. Where a significant amount of sensitive information must be sent by mail consider utilising either a secure courier service or, more likely, Royal Mail Special Delivery.
- When necessary, ask the recipient to confirm receipt.

## C. Communication by email

- Bear in mind that compromise of organisations' email is now a fairly well-established risk. It is a fair assumption that any information sent by email is unlikely to be completely deleted and that the information stored by others will be a target for fraudsters.
- Transfer of sensitive personal information by email should be avoided unless the information is sent as an encrypted attachment.
- Consider the probable security of the recipient, for example information sent to a large organisation such as the NHS is likely to be held in considerably more securely on receipt, than information sent to

a volunteer who has an ordinary web-based email. Their devices are less likely to be compromised, and they are more likely to have proper procedures in place for the destruction of information.
- If identifiable information must be sent it MUST be encrypted
- The email header should make it clear that the information contains confidential information.

D. **Communication by SMS and other messaging services**

- Transfer of information using SMS is quick and convenient, and there are times when being able to send a message to someone's mobile telephone is a good way of reaching them 'in the field'. If staff are considering using this method then particular attention should be given to abiding by the principle of sending the minimum information necessary, such as asking the recipient to call the sender back on receipt of the message.
- Other messaging applications may from time to time be considered to be appropriate by staff. Where staff are considering the use of other applications of this type similar attention should be given to only sending messages in which the confidential information is kept to an absolute minimum.
- There are a wide variety of messaging applications available and there are few hard and fast rules about the mechanics of the transfer of information within the different systems. It is staff's responsibility, if using a messaging system which they have not been specifically asked to use by their line manager, to ensure that they understand the peculiarities of the system in question and, if necessary, seek guidance from a manager or more likely from the IT Officer.
- When communicating with individuals by any means which is likely to be received on a mobile device staff should only send messages about which there would be no concern if read by others since these messages are unlikely to be deleted absolutely from a phone or tablet.

**E. Transfers you might not think of.**

There are a number of other processes which give rise to a transfer of information, which one would not immediately recognise as such.

- **Use of home computers or mobile devices to access Volunteer Cornwall systems**. While secure connections can be made to Volunteer Cornwall systems there is an argument that, by accessing the information held by Volunteer Cornwall, through your own machine it has been transferred (even if you only use your computer to work on a remote desktop and the data itself never leaves the control of Volunteer Cornwall's servers). When using their own device staff cannot rely on the protections of Volunteer Cornwall

  For this reason remote access will be granted such access where there is a genuine need for access from home which is agreed with the relevant manager, where such a genuine need exists and is likely to manifest itself consideration will be given to providing a device capable of such access over which Volunteer Cornwall retains control.

- **Storage of information on portable storage media.** The use of portable storage media, such as USB sticks, to transport large quantities of data can also be considered analogous to a 'transfer'. While such drives are likely to be retained by staff and the data is not strictly transferred to another organisation or person the information has been stored in circumstances which effectively move it beyond the physical control of Volunteer Cornwall. Such storage media is capable of being removed easily from the office and can store huge quantities of data and the use of such devices should therefore be considered along the same principals. For example, a back-up copy of a database should not routinely be taken off-site without it being a formally agreed contingency measure.

Signed:  Date: 2nd February 2023

Ian Jones
Chief Executive
For Volunteer Cornwall

Review due: 04/24