# Secure Handling of Disclosure Information

## Background, guidance and what you need to consider

The purpose of the Secure Handling policy is to give instructions on how to appropriately handle disclosure records (referred to in this document as disclosures) and to provide assurance to Volunteer Scotland Disclosure Services (VSDS) and to your paid staff and volunteers that their disclosure information will be handled, used, stored and destroyed appropriately and in accordance with the Disclosure Scotland Code of Practice.

The majority of the disclosures issued will be sent to your organisation by email and only those disclosures that Disclosure Scotland need to print will be passed to your organisation either by post or by telephone results. Telephone results are only available for organisations who are not able to receive or securely store paper certificates. For this reason, you need to consider storage of digital disclosures and either paper disclosures or telephone results.

Keeping an accurate tracking record of the disclosures your organisation has requested and received will be essential and if you are keeping the disclosures, you will need to record whether you received a digital copy, a paper copy or a telephone result. This will allow you to find the disclosure more easily when the time comes to destroy or delete it. A Microsoft Word version of the Disclosure Tracking Record can be found at the end of this document, or a Microsoft Excel version can be downloaded from the resources section of our website.

Organisations may struggle with the secure storage of digital disclosures and need to consider what will happen when there are changes of signatories or those who are responsible for the disclosure process. Organisations have different options for saving the digital disclosure and you need to carefully consider the best way to store, restrict access and delete digital disclosures. Organisations may find practical to delete or destroy disclosures once the recruitment decision has been made at which point the disclosure serves no other purpose. The only exception is where organisations are providing transport services for health or education services (they will need to retain their digital disclosures until the scheme member leaves their role).

## Storing and accessing disclosure information

If your organisation has a shared drive or workspace and IT support who can arrange an area on your network to store digital disclosures, this will be the most secure option.  IT should be able to restrict access to those that are entitled to see disclosure information.  Using this type of storage will mean that there is reduced risk of you losing access to disclosures if a signatory leaves.

What you need to consider and manage is that there may be several people entitled to see disclosure information relevant to recruitment processes they are overseeing but not entitled to see disclosures for recruitment in other areas of your business.

If the signatory leaves, IT can arrange for another person to have access to the storage area.

## Cloud storage

This can be used in a similar way to network storage where organisations don't have a network or IT support who can set up restricted access.  Using cloud storage like Dropbox, Google, Teams, I Cloud etc will allow you to set up restricted access to disclosures.  If you've not set up this type of document sharing or storage before, save a test document and check that only the right people have access to it.

At least two people should have the log in details or ability to access the cloud storage which will mean that if one person leaves, there is someone else who has access, and you will not lose or be locked out of the stored disclosures.

## Local device

Using a device like a PC, laptop, mobile device or pen drive to store disclosures may seem secure, however, there are risks:

- Your organisation could be left with no access to the device, or you may find you're locked out of the device, when a signatory moves on.
- If equipment is shared by several members of staff, you need to consider who has access to information
- on that shared device.

- You should also consider the impact of loss, theft and data corruption in using a single device to store important information. For example, pen drives are easily lost.

Any device you use should be password protected and safely stored. If access cannot be guaranteed you should consider other ways of handling disclosure information.

## Receiving or storing disclosure information through email

If you are using a shared email address, you must take steps to ensure anyone with access to the shared email is entitled to see disclosure information.  Consider setting up a new email account to receive disclosures if secure access cannot be guaranteed.

If using an email account to store certificates, you should consider the issues this creates for secure access, safe storage and retention. You should consider how disclosures will be accessed from an email address if the signatory leaves the organisation. If a signatory is using their personal email address to store certificates, it is unlikely that the organisation will be able to access the disclosures after the signatory has left. If the signatory is forwarding the emails with disclosures to another signatory before leaving, it is essential that the outgoing signatory deletes all copies of the disclosures from their inbox and their sent items. The signatory receiving the emails should follow the appropriate steps as outlined above.

Regardless of which approach you take, especially as a small business or organisation, you must consider Cyber Security. The National Cyber Security Centre provides good advice and next steps in this area **https://www.ncsc.gov.uk/collection/small-business-guide**.

## Print a copy

If none of the digital storage options are suitable and you need to keep a copy of the disclosure, you can print a copy and store it as you would store a paper certificate issued by Disclosure Scotland.  This should only be done if you need to keep a copy. If printing a copy, you need to delete any digital copies.

## Retain one copy only

When considering how to store your digital disclosures, you should remember that only **one copy** should be stored. This will make handling the disclosure information easier.  Remember that if you are forced to download a copy to view it, this will be automatically saved in the downloads folder on your device. This downloaded copy and the email will need to be deleted once you have saved a copy to your chosen place.

Given the challenges in storing digital disclosures, consider whether you really need to keep a copy.  It may be easier and safer to delete the digital disclosure once you've reviewed it and made your recruitment decision.

## Lost disclosures

If you lose a physical or digital copy of a disclosure, you must contact VSDS immediately to let us know.  This includes if a storage device like a pen drive or laptop that disclosures are saved on is lost or stolen or where a signatory has used their own device and has not given alternative access when they leave your organisation.  You will also need to refer to your GDPR policy and guidance from the Information Commissioners Office **ICO Report Personal Data Breach** for further guidance on other steps you may need to take.

## How to use this policy

Using the information and guidance in the first four pages of this document, you need to decide how you will store digital certificates.

Once you have decided on the best process for your organisation, you should detail this, where indicated, in the digital certificates section of the policy below.

### Email Received with Digital Certificate

- Who has access to this email address?
- If using a shared email address, what steps can you take to restrict access to digital disclosures?
- Consider setting up a new email address to receive confidential information.
- Don't forget to keep VSDS updated with new email addresses!

### Review

- Details correct?
    - Share with those that need to see the disclosure
    - Make recruitment decision
    - Record decision

- Incorrect details on disclosure?
    - Applicant to contact Disclosure Scotland.  Await outcome of review.

## Sharing Information

- Who else needs to see the disclosure?
- How will you share the disclosure?
- Does anyone who has access to disclosures understand they need to comply with the code of practice?
- If sharing by email, does the person you're sharing with know to delete after reviewing?
- Take care to enter the correct email address if sending by email.  Refer to your organisations's GDPR policy in instances where disclosures are sent to someone in error.

## Record Keeping

- Record decision on tracking record.  A copy of the tracking record can be found in the resources section of our website.
- Record whether the disclosure is digital or paper to allow you to locate it when it's time to destroy or delete it

## Retention

- Do you need to keep the digital disclosures?
- Remember that they can only be used for the purpose they were issued for.
- If you don't need to keep them, delete them.  You'll still have a record of them in you tracking record.

## Storage

- Network - This is the most secure option for organisations with IT support.
- Cloud - This is the most secure option for organisations without IT support.
- Local Device - Care should be taken with shared devices or email addresses that no one else has access to the disclosures. The signatory must ensure the organisation still have access to disclosures if they leave.
- Email - As above for local device
- Pen Drive - These carry the greatest risk. Pen drives are small and easily lost.  The pen drive should be stored securely and password protected.
- Paper - digital disclosures can be printed and stored as you would store paper disclosures received.

## Deletion

- Digital disclosures should not be retained for longer than the scheme member is in regulated work with your organisation.
- Ensure anyone that you sent a copy of the disclosure to deletes all copies including the email, saved copies and any copy that is automatically saved in download folders or automatically backed up.

## Responsibility

- It is your organisations responsibility to ensure you are handling, storing  and deleting digital disclosures appropriately.
- If you are storing disclosures with passwords, ensure more than one person has the password information to ensure your organisation is always able to access them.
- Consider creating a handover pack with all the information a new Lead Signatory/Collator would require.
- If you need help or advice, please contact our Training and Compliance Team by calling 01786 849777 (option 3) or email **disclosures@volunteerscotland.org.uk**

# Secure Handling of Disclosure Information Policy

## (ORGANISATION NAME)

The purpose of this policy is to provide guidance and instruction on how to appropriately handle disclosures for those who will have access to them and to provide assurance to Volunteer Scotland Disclosure Services and our staff and volunteers that their disclosure information will be handled, used, stored and destroyed appropriately and in accordance with the Disclosure Scotland Code of Practice.

For the purpose of this policy, PVG Scheme Records, PVG Scheme Record Updates, Standard and Enhanced disclosures will be referred to as disclosures.

This policy is for organisations enrolled with Volunteer Scotland Disclosure Services to access disclosures for the purpose of assessing individual's suitability for paid and/or voluntary work.

In accordance with the Scottish Government Code of Practice, for registered persons and other recipients of disclosure information, we will ensure the following practice.

## Requesting Disclosures

Disclosures will only be requested when necessary and relevant to a particular post and the information provided on a disclosure will only be used for recruitment purposes.

Our organisation will ensure that an individual's consent is given before seeking a disclosure. Before using disclosure information for any other purpose, we will seek their consent and will take advice from VSDS to ensure it is appropriate to use the disclosure for a purpose other than recruitment. Furthermore, we will ensure that all sensitive personal information that is collated for the purposes of obtaining a disclosure will be always managed confidentially by those involved in the disclosure process.

## Sharing Information

Disclosure information will only be shared with those authorised to see it in the course of their duties.

## Storage

Disclosure information will be stored in secure conditions as follows:-

## Digital Certificates

Care will be taken in relation to electronic disclosure information, and we will endeavour to prevent unauthorised viewing, transmission, storage, printing or fraudulent manipulation.

Access to digital certificates will be restricted to those who are entitled to see it in the course of their duties.

**Insert details of how you will store digital disclosure records here:**

No photocopy or other image of the disclosure information will be retained.

## Paper Disclosures

Paper documents will be kept in lockable and non-portable storage units. Access to disclosure information will be restricted to those that are entitled to see it in the course of their duties.

No photocopy or other image of the disclosure information will be retained.

## Telephone Results

When receiving disclosure information by telephone, VSDS staff will only convey information detailed in disclosures accessed by our organisation to our enrolled signatories once they have correctly answered the relevant security questions.

Failing to provide the correct answers to the required security questions will result in VSDS withholding the required information and may lead to an investigation being carried out to establish why our enrolled signatory was unable to provide the required security information.  Once the disclosure information has been shared with us, VSDS will shred the disclosure.

VSDS does not keep a record of any information contained on the disclosure.  When receiving a telephone result, it is essential that we record the information required for our Disclosure Tracking Record.

Further advice about secure handling can be found in the code of practice.

## Record Keeping

It is our organisations responsibility to keep accurate information about disclosures we have accessed. The following information will be recorded on our Disclosure Tracking Record:

- Date of issue of disclosure
- Name of subject
- Disclosure type/level
- Unique reference number of disclosure
- Position for which the disclosure was requested (please note this will no longer be detailed on the digital disclosure)
- Whether we received a digital or paper disclosure or if we received the information by telephone
- Where the disclosure is stored
- Recruitment decision taken

We will not record whether there was any vetting information as the code of practice prohibits this.

## Retention

We will not retain disclosures for longer than is necessary for the purpose for which the disclosure record was obtained. PVG disclosures will be destroyed securely on receipt of an updated PVG disclosure, and they will not be retained beyond the last day that a scheme member is carrying out regulated work for our organisation.

## Destruction/Deletion

We will take reasonable steps to ensure that disclosure information is destroyed by suitable and secure means, for example, shredding, pulping or burning. Electronic images from digital certificates will also be deleted permanently from both the email address where it was received and from where it is stored.

We will ensure that all staff with access to disclosure information are aware of this policy and have received training and support to help them to comply with both this policy and the code of practice.  A copy of this policy will be made available to any applicant, member of staff or volunteer who requests it.

# (Organisation Name)

## Disclosure Tracking Record

| Details of application form | | | | | | | | Disclosure Certificate | | | | Recruitment Decision | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Name of Applicant | Date of Birth | Level of Disclosure | Position | Signatory | Date Requested | Email/ Paper form | Date Recorded | Certificate Number | Membership Number | Digital/ Paper copy stored | Date Destroyed | Yes/ No | Date |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |