Secure Handling of Disclosure Information Policy - Guidance

Before using this policy template, you must consider the following guidance and update your existing practices accordingly.

All organisations are required by the Code of Practice to have a secure handling policy in place to detail how disclosure information will be handled, used, stored and destroyed/deleted. With a new way to view disclosure information from 10 June 2024, organisations need to consider how to handle disclosure information provided in up to 4 different ways.

- Online results
- Paper disclosures
- Telephone results (only available for organisations who are not able to receive or securely store paper certificates)
- Emailed disclosures (these will no longer be issued but storage of previously issued email disclosures still needs to be considered and detailed in the policy)

From 10 June 2024, the majority of the disclosures issued will be online results and email disclosures will no longer be issued. When the applicant receives their copy of the disclosure, they will then need to approve your organisations access to the information. In most cases, the applicant will give your organisation digital access to view online results. This means a link will be sent to the email address provided on the online application request form, to allow your organisation to view the online result.

There may also be circumstances where Disclosure Scotland need to issue a paper copy of the disclosure. When we receive a paper disclosure for your organisation, we will either send this to you by post or provide the information as a telephone result (where you're registered for this service).

As you will no longer have a copy of the disclosure where online results have been issued to you, keeping an accurate tracking record of the disclosures your organisation has requested and received will be essential. You will need to record whether you received an online view, email copy, a paper copy or a telephone result. You will also need to keep accurate records showing if the email or paper copies have been destroyed or stored so that you know if you need to destroy/delete the disclosure when applicants move out of regulated work with your organisation. A PDF and a Microsoft Excel version of the Disclosure Tracking Record can be downloaded from the guidance and resources section of our website to help you keep a record of the disclosures you've requested.

You should continue to detail how you are storing any previously emailed disclosure information in your secure handling policy (unless you have deleted them and do not store copies). The details of how you store and destroy emailed certificates will need

to be copied over from the previous copy of the Secure Handling Policy if you intend to continue to store them.

Secure Handling of Disclosure Information Policy for the Tain and North Highland YMCA SCIO

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 Short Scheme Records, Standard disclosures 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.

We will not request disclosure information for other organisations without first discussing the appropriate process and receiving approval for this from VSDS.

Sharing Information

We will only share disclosure information with those authorised to see it in the course of their duties.

Storage

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

- **Online Results**

A note will be taken of any vetting information which needs to be reviewed. Access to disclosure information will be restricted to those that are entitled to see it in the course of their duties. When receiving an online result, it is essential that we record the information required for our Disclosure Tracking Record.

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. This Lockable Filing Cabinet is kept within the main YMCA office 17, Stafford street Tain Ross-shire IV191AZ

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.

- ## Emailed Certificates

VSDS ceased emailing disclosures on 10 June 2024, this section is only required for organisations that received disclosures by email and stored those email disclosures.

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

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

Insert details here of how you will store email disclosure records here: (this should be copied from the last version of your Secure Handling Policy).

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

- ## 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:

- Name of Applicant
- Date of Birth
- Level of Disclosure
- Position applied for
- Signatory
- Date Posted/requested online
- Date Processed (application requests only)
- T Reference Number
- Date disclosure issued
- Certificate/Disclosure Number
- PVG Membership Number
- Date Destroyed/Deleted
- Recruitment Decision and date

We will not record whether there was any vetting information as the Code of Practice prohibits this. VSDS provides a sample tracking document in the guidance and resources section of their website.

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 email 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.

Lost Disclosures

If we lose a physical or emailed copy of a disclosure or any other record of disclosure information, we will notify the scheme member(s) affected, VSDS and the Information Commissioners Office.

Code of Practice

Further instructions and guidance on secure handling of disclosure information can be found in sections 17 to 23 of the Code of Practice and 71 to 100 of the Annex to the Code of Practice.