HS07-P02 SECURE HANDLING OF DISCLOSURE INFORMATION POLICY

VERSION CONTROL

Version No.	Date Amended	Amended By	Reason
1.0	18/11/2021		Added to Policy Matrix
2.0	01/07/2023	Risk & Compliance Sub-Committee	Reviewed in line with legislation changes
3.0	20/03/2024	Risk & Compliance Sub-Committee	Minor amendment

Scottish Squash Limited

Secure Handling of Disclosure Information Policy

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 Disclosure Scotland (DS) 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 DS, either directly or via Scottish Squash Limited (SSL), 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 DS 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.

We will not store digital certificates other than for any such period that is required to assess any vetting information that needs to be considered.

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, DS staff will only convey information detailed in disclosures accessed by our organisation to our enrolled signatories.

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); and
- 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.