Correct handling and safekeeping of DBS certificate information

POLICY STATEMENT

Council of the ISLES OF SCILLY

January 2017

Revisions to Source Document

Version	1.1	Approving Committee	Not applicable
Date	January 2017	Ratified by Council	Not applicable
Responsible Officer	Theo Leijser, Chief Executive Officer	Review Date	31/01/2020

Version History

Date	Version	Author/Editor	Comments
16/01/17	1.0	Joseph Payne	Final draft
23/01/17	1.1	Bob Dawson	Formatted

Equalities Impact Assessment Record

Date	Type of Assessment Conducted	Stage/Level completed (where applicable)	Summary of Actions Taken Decisions Made	Completed by.	Impact Assessment Review date

Document retention

Document retention period	

CONTENTS

If you require this document in an alternative language, in larger text, Braille, easy read or in an audio format, please contact the Council at diversity@scilly.gov.uk or telephone 01720 424000

Introduction

1.1 As an organisation using the Disclosure and Barring Service (DBS) checking service to help assess the suitability of applicants for positions of trust, the Council of the Isles of Scilly complies fully with the code of practice regarding the correct handling, use, storage, retention and disposal of certificates and certificate information.

1.2 It also complies fully with its obligations under the Data Protection Act 1998 and other relevant legislation pertaining to the safe handling, use, storage, retention and disposal of certificate information and has a written policy on these matters, which is available to those who wish to see it on request.

Storage and access

2.1 Certificate information should be kept securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties.

Handling

3.1 In accordance with section 124 of the Police Act 1997, certificate information is only passed to those who are authorised to receive it in the course of their duties. We maintain a record of all those to whom certificates or certificate information has been revealed and it is a criminal offence to pass this information to anyone who is not entitled to receive it.

3.2 To note: those registered care homes which are inspected by the Care Quality Commission (CQC), those organisations which are inspected by Ofsted and those establishments which are inspected by the Care and Social Services Inspectorate for Wales (CSSIW) may retain the certificate until the next inspection.

3.3 Once the inspection has taken place the certificate should be destroyed in accordance with the code of practice.

Usage

4.1 Certificate information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

Retention

5.1 Once a recruitment (or other relevant) decision has been made, we do not keep certificate information for any longer than is necessary. This is generally for a period of

up to six months, to allow for the consideration and resolution of any disputes or complaints.

5.2 If, in very exceptional circumstances, it is considered necessary to keep certificate information for longer than six months, we will consult the DBS about this and will give full consideration to the Data Protection and Human Rights of the individual before doing so.

5.3 Throughout this time, the usual conditions regarding the safe storage and strictly controlled access will prevail.

Disposal

6.1 Once the retention period has elapsed, we will ensure that any DBS certificate information is immediately destroyed by secure means, for example by shredding, pulping or burning. While awaiting destruction, certificate information will not be kept in any insecure receptacle (e.g. waste bin or confidential waste sack).

6.2 We will not keep any photocopy or other image of the certificate or any copy or representation of the contents of a certificate. However, notwithstanding the above, we may keep a record of the date of issue of a certificate, the name of the subject, the type of certificate requested, the position for which the certificate was requested, the unique reference number of the certificates and the details of the recruitment decision taken.

Acting as an umbrella body

7.1 Before acting as an umbrella body, we will take all reasonable steps to ensure that third parties are aware of the Data Protection Principles and provide them with guidance on secure handling and storage of information.

Annex 1. References

Sample policy on the handling of DBS certificate information. DBS. 14 November 2012

Revised Code of Practice for Disclosure and Barring Service Registered Persons. Home Office. November 2015

Annex 2. Data protection principles

Schedule 1 to the Data Protection Act lists the data protection principles in the following terms:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
   (a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.