



## **Handling and Safekeeping on DBS Certificate Information**

### **General principles**

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

It also complies fully with its obligations under the General Data Protection Regulation (GDPR), Data Protection Act 2018 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**

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**

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.

*To note: those organisations which are inspected by Ofsted may be legally entitled to retain the certificate for the purposes of inspection.*

In addition, organisations that require retention of certificates in order to demonstrate 'safer recruitment' practice for the purpose of safeguarding audits may be legally entitled to retain the certificate. This practice will need to be compliant with the Data Protection Act, Human Rights Act, General Data Protection Regulation (GDPR), and incorporated within the individual organisation's policy on the correct handling and safekeeping of DBS certificate information.

### **Usage**

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**

Once a recruitment (or other relevant) decision has been made, we do not keep certificate information for any longer than is necessary. This retention will allow for the consideration and resolution of any disputes or complaints, or be for the purpose of completing safeguarding audits.

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

### **Disposal**

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).

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.

**Retention of records relating to allegations against adults who are or have been working in the setting:**

Record retention info below from NSPCC states:

Keep the records in their personnel file either until they reach the age of 65 or for 10 years whichever is longer (IRMS, 2016). This applies to volunteers and paid staff.

For example:

- if someone is 60 when the investigation into the allegation is concluded, keep the records until their 70th birthday
- if someone is 30 when the investigation into the allegation is concluded, keep the records until they are aged 65.

You should keep records for the same amount of time regardless of whether the allegations were unfounded. However, if you find that allegations are malicious you should destroy the record immediately.

Information should be kept for this length of time even if the person stops working or leaves the setting .

**Links:**

<https://learning.nspcc.org.uk/media/1442/child-protection-records-retention-and-storage-guidelines-oct-2018.pdf>

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/741314/Keeping\\_Children\\_Safe\\_in\\_Education\\_\\_3\\_September\\_2018\\_14.09.18.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/741314/Keeping_Children_Safe_in_Education__3_September_2018_14.09.18.pdf)

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>

**DBS service update Feb 2019**

Organisations should not keep the original paper certificate. This is the employee's property. They must return the certificate to the employee once they have checked it.

Employers can make a copy of a certificate. This is as long as they have permission from the employee. If you have this, there is no official time limit for keeping the copy.

All organisations should have a policy on storing personal information. This policy should meet the requirements of the General Data Protection Regulation (GDPR).

Visit the Information Commissioner's Office website. You will find details on how employers should handle personal information there.

***The Disclosure and Barring Service***

***PO Box 165, Liverpool, L69 3JD Call Centre: 03000 200 190***

This policy was adopted by \_\_\_\_\_ (name of provider)

On \_\_\_\_\_ (date)

Date to be reviewed \_\_\_\_\_ (date)

Signed on behalf of the provider \_\_\_\_\_

Name of signatory \_\_\_\_\_

Role of signatory (e.g. chair, director or owner) \_\_\_\_\_

