South Farnham School
DBS Registered Body
Handling of Disclosure Information Policy

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, South Farnham School 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 GDPR and 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.

Scope

It is the responsibility of all staff to take care when processing DBS data to avoid data breaches and/or falling foul of the legislative requirements of the GDPR.

A data breach can happen if:

- Data is lost.
- Data is accessed without authorisation or without proper legal right/permission to do so.
- Data is disclosed or acquired without authorisation or without proper legal right/permission to do so.
- Data is destroyed unlawfully.
- Data is not maintained securely.
- Confidentiality of data is not maintained.
- Protections put in place to maintain data including technical, organisational and administrative safeguards are ignored, undermined and not adhered to.

Any loss of data or personal data can have serious effects for individuals and/or institutions concerned. Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in current relevant data legislation and regulations.

Storage and access

Certificate information is 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.

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 is generally for a period of up to six months, to allow for the consideration and resolution of any disputes or complaints, or be for the purpose of completing safeguarding audits.

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.

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

The only exception to the above is where a document has also been used to verify an individual's right to work in the UK eg passport. A copy of such information must be kept on the employee's personal file.

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, not withstanding 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

As an umbrella body (an umbrella body being a registered body which countersigns applications and receives certificate information on behalf of other employers or recruiting organisations), we will take all reasonable steps to satisfy ourselves that they will handle, use, store, retain and dispose of certificate information in full compliance with the code of practice and in full accordance with this policy.

We will also ensure that any body or individual, at whose request applications for DBS certificates are countersigned, has such a written policy and, if necessary, will provide a model policy for that body or individual to use or adapt for this purpose.

Data breaches

The GDPR requires that we notify the ICO and, in some circumstances, the data subject of any personal data breaches within 72 hours of becoming aware of the breach.

We have put in place protocol to deal with any suspected personal data breach and will notify the appropriate personnel where it is necessary to do so.

The GDPR states that personal data must be processed in accordance with the data protection principles. Staff must adhere to and be committed to these principles as follows:

- We process personal data lawfully, fairly and in a transparent way.
- We collect personal data only for specified, explicit and legitimate purposes.
- We process personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- We keep accurate personal data and take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- We keep personal data only for the period necessary for processing.
- We adopt appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, accidental loss, destruction or damage.
- In our privacy notices, we tell individuals the reasons for processing their personal data, how we use such data and the legal basis for processing. We will not process personal data of individuals for reasons other than the stated purpose or purposes.
- Where we process special categories of personal data or criminal records data to perform obligations, this is done in accordance with a policy, or for legal reasons. We will update personal data promptly if an individual advises us that his/her information has changed or is inaccurate.

Consent

Consent is one of the lawful grounds by which personal data can be processed. Consent must be fully informed and unambiguous meaning that the data subject must be clear as to what they are consenting to and the reasons for it. Particular care must be taken when processing special categories of personal data because a higher threshold is required for such information.

Consent will only apply in some specific circumstances because the other lawful grounds are usually more appropriate when processing the personal data of pupils, parents, guardians and staff.

Consent should be in writing so that it can be evidenced at a later stage. Consent can be withdrawn at any time. Fresh consents must be obtained if the personal data it covers, or the purpose for processing, becomes invalid or incompatible with the new processing requirements.

If you believe that consent is required for you to process certain types of personal data and you do not have it, or you do not believe it is clear and unambiguous, you must obtain it before carrying out the processing. You must speak to the DPO if you are unclear about this requirement or need assistance.

Privacy notices

Obligations under the GDPR include providing specific information to data subjects on the information that we collect, retain and generally process. This requirement is to be transparent in the way we process personal data.

Transparency means that we are required to specify the purposes for which we process personal data, how long we may hold the information for and what the data subject's rights are.

We have included this information within the school's DBS Registered Body privacy notice.

Crucially, we are not allowed to process personal data for a purpose that is incompatible with one of the stated purposes in our privacy notice. While we have sought to identify all the purposes for which we process personal data in our privacy notice it may be that the stated purposes have to be extended in certain circumstances. Any issues that arise in relation to this should be referred to the DPO.

Accuracy

To comply with the data protection principles we must ensure that personal data is accurate and, where necessary, kept up-to-date.

Where data is not accurate it must either be corrected or deleted straight away.

Staff members are required to check the accuracy of the personal data they process and, when any errors or issues arise, they must take all reasonable steps to resolve them.

Data security measures: integrity and confidentiality

One of the principles of the GDPR is to maintain the integrity and confidentiality of personal data.

Information security is at the forefront of the GDPR's key requirements. Every aspect of data security must be considered with technological and administrative processes being key to avoiding threats to the security of personal data. Appropriate security measures must be implemented that are appropriate to the risks to the data.

- The schools will encrypt any data that is determined to be personal or commercially sensitive in nature. This includes data held on fixed station computers, laptops, portable devices and memory sticks.

- All staff will be trained to understand the need to handle data securely and the responsibilities incumbent on them.

- The Trust has a clear policy and a procedure for the use of cloud-based storage systems and is aware that data held in remote cloud storage is still required to be protected in line with the GDPR. The Trust will ensure that it is satisfied with the controls put in place by service

providers to protect the data. (See the DfE document Cloud software services and the Data Protection Act 2014 www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act.)

- Staff should *not* copy or remove special categories of personal data or commercially sensitive data from the school or authorised premises unless the media are:
    - Encrypted.
    - Transported securely.
    - Stored in a secure location.
- Sensitive data *should not* be transmitted in unsecured emails.
- Data transfer should be through secure websites..
- Data must be automatically backed up, encrypted and stored in a secure place – eg safe/fire safe/remote backup facility.
- All staff computers, including laptops, must be used in accordance with the policy for ICT and use of the internet and intranet by staff.
- When laptops are passed on or re-issued, data will be securely wiped from any hard drive before the next person uses it (not simply deleted). This will be done by the school's ICT technical support staff.
- The school's wireless network (wifi) will be secure at all times.
- Devices that are not the property of the school should only be used in line with our policy on the use of personally owned devices by staff.
- The school will ensure that staff who are responsible for processing DBS information know what data is held, who has access to it, how it is retained and how and when it is disposed of.
- Where a member of the school has access to data remotely, the remote access off the school site to any personal data should be over an encrypted connection (eg VPN) protected by a username/ID and password. This MIS information/school data must not be stored on a personal (home) computer.
- The school will keep necessary information in accordance with the Information and Records Management Society's (IRMS) guidance and the records retention policy.
- The will securely delete commercially sensitive or personal data when it is no longer required according to the IRMS's guidance and the records retention policy.

Data should remain confidential and you should not share it with any unauthorised personnel or third parties.

Obligations under this policy

The purpose of this policy is to advise all members of staff what is required by South Farnham School DBS Registered Body to ensure that it complies with the GDPR at all times and to advise all members of staff how to proceed when handling data which needs to be handled securely.

……