DATA PROTECTION AND SECURITY

Definitions that relate to this section only are:

personal data	is information that affects a person's privacy. It is about a living person who can be identified from the data. It need not be sensitive information and can be as little as a name and address.
sensitive personal data	is information concerning a person's racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, membership of a Trade Union, physical or mental health conditions, sexual life, commission or alleged commission of any offence, a record of any proceeding for any offence committed or alleged, or a record of any sentence or proceedings.

Data Protection Act 1998

The Act seeks to protect an individual against the unfair use of personal information and sets out the following three fundamental principles:

- The right of an individual to know what data is being held and to check its accuracy;
- That *personal data* should be recorded only for the specific purposes for which it is held and should not be disclosed to those not authorised to have it; and
- A Government agency with a Data Protection Registrar should regulate and enforce proper standards relating to *personal data*.

There are eight principles laid down in the Act, which set out the rules for dealing with *personal data*. These are:

1. *Personal data* must be processed fairly and lawfully.
2. *Personal data* shall be obtained only for one or more specified and lawful purposes and shall not be processed in any manner incompatible with that purpose or purposes.
3. *Personal data* shall be adequate, relevant and not excessive in relation to the purpose or purposes for which the data has been obtained.
4. *Personal data* shall be accurate and where necessary kept up-to-date;
5. *Personal data* shall be held no longer than is necessary for the purpose for which the data has been obtained.
6. *Personal data* shall be processed in accordance with the rights of *data subjects* under the Act.
7. Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of *personal data* and against accidental loss or destruction 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.

Secure storage, handling, retention and disposal of all *personal data*

1. **Storage:** *sensitive personal data* must always be kept separately and securely and in a lockable storage container with access strictly controlled and limited to those who are entitled to see it as part of their duties.

3. **Handling:** In accordance with Section 124 of the Police Act 1997, Disclosure 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 Disclosures or Disclosure information has been revealed and recognise that it is a criminal offence to pass this information to anyone who is not entitled to receive it.

4. **Usage**: Disclosure information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

5. **Retention: Disclosure information will be held by the designated persons at SSDC and Child-Safe.** Once a recruitment (or other relevant) decision has been made Disclosure information will not be kept 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. If, in very exceptional circumstances, it is considered necessary to keep Disclosure information for longer then six months, the designated persons will consult the CRB and will give full consideration to the data protection and human rights of the individual subject to access requirements before doing so. Throughout this time the usual conditions regarding the safe storage and strictly controlled access will prevail.

6 **Disposal**: All *personal data* will be destroyed by secure means, e.g. shredding, pulping or burning. While awaiting destruction, sensitive personal data will be retained in its secure file. We will not keep any photocopy or other image of the Disclosure or any copy or representation of the Disclosure. However, we may keep a record of the date of issue of a Disclosure, the name of the *data subject*, the type of Disclosure given, the position for which the Disclosure was requested, the unique reference number of the Disclosure and the details of the recruitment decision taken.