

# **Data Protection Policy**

## **The Association for Pastoral Supervision and Education**

Last updated 22nd June 2018

### **Definitions**

GDPR The General Data Protection Regulation

**Responsible Person** Ms J Walker

**Register of Systems** means a register of all systems or contexts in which personal data is processed by the Charity.

### **1. Data protection principles**

The Association for Pastoral Supervision and Education (APSE) is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

- a. processed lawfully, fairly and in a transparent manner in relation to individuals;
- b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
- f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

### **2. General provisions**

- a. This policy applies to all personal data processed by APSE.
- b. The Responsible Person shall take responsibility for APSE's ongoing compliance with this policy.
- c. This policy shall be reviewed at least annually.
- d. APSE shall register with the Information Commissioner's Office as an organisation that processes personal data.

### **3. Lawful, fair and transparent processing**

- a. To ensure its processing of data is lawful, fair and transparent, APSE shall maintain a Register of Systems.
- b. The Register of Systems shall be reviewed at least annually.
- c. Individuals have the right to access their personal data and any such requests made to APSE shall be dealt with in a timely manner.

#### **4. Lawful purposes**

- a. All data processed by APSE will be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.
- b. APSE shall note the appropriate lawful basis in the Register of Systems.
- c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
- d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in APSE's systems.

#### **5. Data minimisation**

- a. APSE shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

#### **6. Accuracy**

- a. APSE shall take reasonable steps to ensure personal data is accurate.
- b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

#### **7. Archiving / removal**

- a. To ensure that personal data is kept for no longer than necessary, the Charity shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
- b. The archiving policy shall consider what data should/must be retained, for how long, and why.

#### **8. Security**

- a. APSE shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
- b. Access to personal data shall be limited to only those personnel who need access, and appropriate security should be in place to avoid unauthorised sharing of information.
- c. When personal data is deleted this should be done safely such that the data is irrecoverable.

#### **9. Breach**

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, APSE shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.

**END OF POLICY**