Data Controller documentation

**Accountability and governance**

**data protection policy (3.1)**

We have a Data Protection Policy.

**monitor compliance with data protection policies and regularly review the effectiveness of data handling and security controls (3.1)**

Documentation is not enough to ensure compliance. Periodic compliance checks should be carried out. This is part of the schedule of tasks.

**provide data protection awareness training for all staff (3.1)**

Provide awareness training on appointment.

**manage information risks in a structured way so that the KS understands the business impact of personal data related risks and manages them effectively (3.3)**

Specify information risks, procedures to mitigate them and an action plan.

**implement appropriate technical and organisational measures to integrate data protection into our processing activities (3.4)**

We need to demonstrate that we have implemented technical or organisational measures to ensure data protection is part of our activities.

We have done so by:

* installing antivirus software on the church PC
* issuing guidance to staff and members of the congregation who hold church data
* keeping areas secure where data is stored via keypads

**understand when we must conduct a DPIA and have processes in place to action this (3.5)**

A Data Protection Impact Assessment (DPIA) is needed when new technologies are introduced for example. The DPIA should contain the following information:

* a description of the processing operations and the purposes including, where applicable, the legitimate interests pursued by your business;
* an assessment of the necessity and proportionality of the processing in relation to the purpose;
* an assessment of the risks to individuals; and
* controls that you put in place to address any risks you’ve identified (including security).

**have a DPIA framework which links to our existing risk management and project management processes (3.5)**

Probably unnecessary

**nominate a data protection leader (3.6)**

To be done

**KS demonstrate support for data protection legislation and promote a positive culture of data protection compliance (3.7)**

The KS should demonstrate its commitment to data protection.