Information risk assessment procedure

1. **Scope**

   This method of risk assessment is applied throughout Canterbury Cross Primary School in respect of all information risks.

2. **Responsible**

   2.1 The information Security Manager and Data Protection Officer are jointly responsible for carrying out risk assessments wherever they are required by the GDPR.

3. **Procedure Step 1 – Identify the risks**

   3.1 The risks to Canterbury Cross Primary School's information are identified by the Information Security Manager, Data Protection Officer and any relevant staff associated with the information under the headings of risks to availability, confidentiality and integrity, and documented in a project risk log.

   3.2 The effect that losses of availability, confidentiality and integrity might have on Canterbury Cross Primary School (i.e. what is the actual harm to the asset itself that might occur) are identified and documented by the Information Security Manager.

   3.3 For each risk, identify the risk owner, which will usually be the person who owns the database or set of records.

4. **Procedure Step 2 – Assess the risks**

   4.1 The impact – the business harm – that might result from the loss of availability, confidentiality or integrity, for each of these risks, is assessed by the Information Security Manager, Data Protection Officer and any relevant staff associated with the information.

   4.2 The realistic likelihood that each of these risks might occur is assessed.

   4.3 The risk levels are assessed.

   4.4 A decision is made, for each of the risks, as to whether it is acceptable or if it must be controlled in line with criteria established by the risk owner.

5. **Procedure 3 – Identify and evaluate options for the treatment of risks**
   5.1 For each of the risks, identify the possible options for treating it in line with the decisions made in 4.4 above.
   5.2 For each of the risks, document which treatment action (i.e. accept, reject, transfer or control) is going to be taken and the reasons for each choice.

6. **Procedure Step 4 – Select control objectives and controls for treatment of the risks**
   6.1 Appropriate control objectives are selected or designed by the Information Security Manager and risk owner, with any necessary advice provided by the Data Protection Officer, according to the specific needs of the risk and the organisation. Controls to achieve those objectives are selected from a variety of appropriate sources.
   6.2 The final selection of controls and control objectives and the reasons for the selections (whether inclusion or exclusion) are documented.

Document Owner and Approval

The Data Protection Officer is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above. A current version of this document is available to all members of staff.

Signature: **Date:**

Change History Record

Issue	Description of Change	Approval	Date of Issue
001		Canterbury Cross Primary School	