ST PETER'S SCHOOL

DATA BACKUP POLICY

2018

1. **Definitions:**
   - School Network – the devices attached to the Network through Data cabling or Wi-Fi.
   - Users – the workforce and students who are given authorised to log on to the School Network.
2. **Introduction:**

   St Peter's will back up all of its data and IT systems on a regular basis to ensure ease of recovery in the event of loss (malicious or accidental) or contamination.

3. **Objectives of Data Backup Policy:**
   - To maintain the integrity of the School's Data.
   - To reduce the risk of cybercrime committed against the school.
   - To reduce the impact and recovery time of the School in response to an IT system failure.
4. **Statement of Intent:**
   - **Fileserver:** All the Data pertaining to the Users of the School network are backed-up daily, at an incremental level, over a 30 day period and held offsite in accordance with the Data Protection Act and GDPR. Current Maximum retention period is 6 months (any changes made before this period will not be able to be recovered).
   - **SIMS:** All the Data contained as part of the School's Information Management System is backed-up daily, at an incremental level, over a 30 day period and held offsite in accordance with the Data Protection Act and GDPR. Current Maximum retention period is 6 months (any changes made before this period will not be able to be recovered).
   - **Vsphere:** All the server infrastructure (Server Farm) is backed-up weekly at an incremental level and held offsite in accordance with the Data Protection Act and GDPR. Current Maximum retention period is 6 months (any changes made before this period will not be able to be recovered).

Created: June 2018

Approved by TLA: 4 July 2018

Ratified by Full Governing Body: 18 July 2018

Due for Review: June 2019