ST PETER'S SCHOOL

USE OF THIRD PARTY SYSTEMS POLICY

2018

Definitions:

* The School – St. Peter's School.

* School's Information Risk Officer (SIRO) – Mr Iain Scott-Brown.

* 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.

* BYOD – Bring your own Device (a device not owned by the School but used to access School digital resources (e.g. Email, Wi-Fi, connect to a computer, remote gateway access)

* ICT Support Team – The staff employed by St. Peter's School to maintain the School's Network and associated systems.

* Staff – the workforce of the School

* User Credentials – Usernames and associated Passwords.

* Third Party Systems – External Systems used by the School to assist in its management and to assist the Teaching and Learning as outlined in the Third Party System Policy.

Introduction:

Staff wishing to use a Third Party System where there is a need to share and store personal data to support the school in its role, whether this is related to the management of the school and its resources or related to the Teaching and Learning of the students – must ensure that the system is fully GDPR compliant. This will be completed through an application process.

Objectives:

* To ensure that the School is fully compliant with the Data Protection Act and the GDPR.

* To minimise the risk of a Data Breach.

Statement of Intent:

Staff may only use these systems once they have received written authorisation from the School's Information Risk Officer.

Authorisation will only occur once the School's Information Risk Officer has worked alongside the applicant to ensure the GDPR is fully complied with.

The member of Staff must complete the necessary form (appendix A) as part of this process. A review of the application should be agreed so that systematic checks may take place. Staff must also inform the School's Information Risk Officer of any changes to service. Any failure to comply with GDPR legislation will lead to the removal of the System.

Updated: June 2018

Approved by TLA 4 July 2018

Ratified by Full Governing Body: 18 July 2018

Due for Review: June 2019