ST PETER'S SCHOOL

BRING YOUR OWN DEVICE (BYOD) POLICY

2018

1. **Definitions:**
    - The School – St. Peter's School.
    - 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)
    - School Community – The workforce and students of the St. Peter's School.
    - ICT Support Team – The staff employed by St. Peter's School to maintain the School's Network and associated systems.

2. **Introduction:**

    The School recognises that members of the School Community may have need to use BOYD whilst at school. In addition, they may also use BYOD to access school systems from home or while mobile (e.g. the remote gateway and Office 365).

    The School accepts NO responsibility for any loss or damage to the device. Furthermore, the ICT Support Team will not be responsible for any maintenance of a BYOD.

3. **Objectives:**
    - To minimise the risk of Personal Data breaches.
    - To minimise the risk of a cyber-attack.

4. **Statement of Intent:**

    BYOD are allowed to connect to the school's Wi-Fi (JOIN) network as long as the device is registered using the Users School Network Credentials.

    In the first instance, BYOD should only use the remote gateway to access/ view personal data. However, it there may be a need to store personal in a file and where this is the case it MUST be encrypted (This includes using Storage Media e.g. USB drives). Please note, the preferred storage place for files containing personal information is the School Network or on Office 365 OneDrive and SharePoint, as these are automatically encrypted.

    Where BYOD are used to access Personal Data via Third Party Systems (e.g. Office 365) they should also have an extra level of encryption (e.g. a pin code or password to access).

    With all BYODs, passwords for school resources and Third Party Systems should not be stored so that other users of the device can access without affirming the associated password.

Updated: June 2018

Approved by TLA: 4 July 2018

Ratified by Full Governing Body: 18 July 2018

Due for Review: June 2019