# Our Lady and St Patrick's
# Roman Catholic
# Nursery and Primary School
# Teignmouth

# Data Protection Policy

**Last reviewed:** **Summer Term 2017**
**Next review:** **Summer Term 2019**
**LGB**

# Our Lady and St Patrick's Roman Catholic Nursery and Primary School
# Data Protection Policy

**Mission:**
The Catholic Faith and the principles of the Gospel are central to the daily life of Our Lady and St Patrick's School. We are committed to:

**"Living, Loving and Learning Together in God's Way"**

**Rationale:**
To ensure that the School: its staff and Governors meet current requirements for data protection.

## Risk Assessment

The School will regularly conduct risk assessments and audits on the identification and storage of personal data which identifies the Information Levels involved. The School has a copy of the Becta Data Handling Guidance which is reviewed by a senior member of staff.

## External organisations and personal data

In rare circumstances, when personal data has to be shared with an outside agency, data subjects have to be made aware of this use through a fair processing notice. Our School will notify the Information Commissioners Office that it processes personal data under the terms of the Data Protection Act.

## Storage and use of personal data

In only very exceptional circumstances, and subject to permission from the Head Teacher, may personal data (including hard copy) be removed from the school premises. In these cases, digital files must be saved in read only format and be password protected, and may only be carried on a single external device and should no account be copied to another external PC or laptop. The file must be deleted when work has been completed.

## Use of school laptops

School laptops may not be used under any circumstances by any non-school staff, they are for the sole use of School staff undertaking work for the school. These laptops must be encrypted.

## Online security

All staff (permanent and temporary) within the school have their own log on and password details to enable them to securely access the IT provision in the School. Upon the termination of their contracts, temporary staff will have these privileges removed. Passwords are changed at regular intervals. The school server is to be physically secured within a locked environment. Appropriate backups are in place, and latest upgrades and patches are applied to the server. Antivirus, anti-spyware and malware software is regularly updated. The School Governors receive information for meetings via e-mail. They are requested to copy this information on to an encrypted memory stick.

**Security good practice**

All staff must follow the basic guidelines for information security. Never leave confidential documents on desks; lock your desk when away from it; always lock sensitive or important documents away; always lock your PC when away from your desk; never use an obvious password (such as sequences of numbers, personal names); inform your line manager if you believe your PC has become infected with a virus, and only use your school internet provision to access trusted sites and sites which are relevant to your work; delete any emails from an unknown origin or that contain odd headings or attachments.

**Wireless access**

Wireless access points within the School are encrypted to WPA2 standard. No non-school laptops are permitted to log onto the internal wireless network, and devices may only be added to the network with the express permission of the Head teacher.

**Incident Reporting:**

Any breaches of security should be reported to the Head Teacher.