



# Laptop/Tablet and Data Protection Policy

## Contents

Data Protection:.....	2
Licensing.....	2
Antivirus.....	3
Housekeeping.....	3
Securing Hardware.....	4
Computer Room.....	4
Classroom.....	4
Pupils' Laptops.....	4
Securing Software.....	5
The Network.....	5
Laptop Computers.....	5
Sen Laptops.....	5
Administration.....	6
Insurance.....	6

## **Data Protection:**

- All teacher laptops are encrypted by Bitlocker.
- All laptops are password protected. It is very important that passwords are not divulged.
- All laptops are password protected. It is very important that passwords are not divulged.
- All files containing sensitive and data in relation to individual pupil's information should be encrypted.
- It is the responsibility of each teacher to back up and secure data on his/her laptop.
- St Joseph's Terenure uses the G Suite platform for storage of Teacher and Student work.
- Data pertaining to pupil data will be stored in the cloud (in Google Drive and through the Aladdin schools Platform).
- Backups of sensitive data will not be stored on USB keys.
- Teachers should log off laptops during breaks and when the laptop is unattended.
- Pupils' classwork is stored in their individual G Suite accounts, which is only accessible to the system administrator and their individual teachers through Google Classroom.
- Group policies prevent changes to computer configuration.

## **Licensing**

- Licensing is overseen by the ICT co-ordinator.
- All software is licensed.
- Licences are stored in the computer room.

## Anitvirus

- St Joseph's Teacher Devices are protected by Windows Defender.
- The PDST (Technology in Education) provides a firewall through the broadband service.
- The PDST will advise if a virus is found on our system.

## Housekeeping

- All application software is stored in the computer room.
- All licences for installed software are stored in the computer room.
- A detailed inventory of all your ICT equipment with all relevant serial numbers and short item description is stored on the network.
- All computers and peripherals are individually labelled for identification.
- Laptop chargers and scanners are labelled.
- All laptops/Chromebooks, cameras, microscopes are stored in the Computer Room when not in use.

## Securing Hardware

ICT hardware is usually secured in either the classroom or the computer room.

Pupils laptops are stored in secure laptop trollies.

Laptops and visualisers are locked using Kensington locks when in use in the classroom

## Computer Room

- The computer room is locked when not occupied
- The computer room is secured with a steel door, bars on all windows and has a motion sensor alarm

## Classroom

- All laptops (teacher and student) should be locked in the classroom using the Kensington lock
- All data projectors are ceiling mounted in the classroom.
- Visualisers are locked using the Kensington locks in the classrooms
- Peripherals such as scanners should be secured in drawers when not in use.

## Pupils' Laptops

- All pupil laptops will be stored in the laptop trolley when not in use. The laptop trolley will be locked at all times
- Laptops will be charged overnight. They will be powered on an electronic timer each night to be charged for use the following day.

## Securing Software

All original media disks are stored in the computer room and should not be removed. Where media is required a backup copy should be used.

## The Network

Hubs and switches for the school network are stored in locked steel cabinets in various locations in the school.

Access to the network servers is password protected.

Each class has a virtual drive on the server for access and storage. This means that other pupils are do not have access to the work from other classes.

## Laptop Computers

All school laptops are stored in the computer room at the end of each day if they are not being brought home by the teacher.

A secure laptop trolley will be in provided for pupils' laptops/Chromebooks.

## Laptops for SEN

- SEN pupils and their parents sign an agreement stating that the laptops are school property and that software may not be installed or uninstalled without ICT Administrator consent.
- Laptops may move to the second level school with the pupils after all licenced software is removed.
- SEN pupils may bring home their laptops when necessary.
- SEN Pupils and their parents sign an agreement regarding appropriate use of devices they have obtained.

## Remote teaching and learning

- It may be necessary to engage in remote learning and teaching in order to maintain continuity of learning.
- Pupils will be facilitated to engage in this process through various methods, including (but not limited to) Teacher correspondence through email, Seesaw, Google Classroom,

and other platforms such as Mangahigh, Thatquiz, Epic Reading, Edpuzzle and WriteReader.

- Parental Consent will be obtained for the use of platforms that require it in line with GDPR.
- The school will endeavour to support those pupils who have difficulties in accessing devices and the internet during remote learning periods.

## **Administration**

The drive and data is shared with the principal only.

Data may be backed up to OneDrive/Google Drive with password protection.

## **Insurance**

The school insurers cover the laptops when in school and when brought outside the school environs by teachers. There is an excess levied in the case of a claim arising.

***Revised by the Board of Management:*** February 2017, reviewed May 2020/April 2021

***Signed by the BOM:***                      ***Fr Philip Bradley***