DATA PROTECTION POLICY
FOR PERSONAL INFORMATION

Version 2 – March 2021

This policy defines how Personal Data is protected at WMAT.

WMAT collects and uses personal information about staff, students, parents, trainee teachers (i2i SCITT) and other individuals who come into contact with the schools.

General guidelines

- Access to Personal Data must only be accessed by authorised employees. Attempts should not be made even if preventative controls are not in place to restrict access.
- Personal Data must not be disclosed to unauthorised people, either internally or externally
- Employees are responsible for protecting Personal Data under their care
- Personal Data must be held if as few places as possible
- Personal Data must be updated when employees are aware of any changes

Personal Data Storage – hard copy

- Personal Data stored in hard copy/paper format is in scope of the General Data Protection Regulation
- Material need to be stored securely when not in use
- Unauthorised people must not have access to printed material
- Material being kept, as part of a data retention schedule, must be done using a managed archive process
- Any material no longer required must be shred as part of an appropriate destruction process.

Personal Data Storage - electronic

- Strong IT controls must be used to secure Personal Data in electronic form:
    - Strong Password must be used
    - Personal Data must not be stored on removable media
    - Personal Data must be stored on appropriately segregated drives
    - PC Screens must be locked when left unattended
- Personal Data should be encrypted when transferring electronically to external parties
- Personal Data must be deleted once it is no longer needed
- All IT assets must be protected using appropriate security software
- Employees must not tamper with or disable security software/controls
- Decommissioning of IT assets must ensure that all Personal Data is removed
- Personal Data must be stored where it can be backed up
- Employees must never create their own copies or versions of Personal Data – Always use and update the master copy of any data
- Employees must not send Personal Data to unauthorised devices
- Employees must not work on Personal Data on unauthorised devices