THOMAS MORE CATHOLIC SCHOOL

ICT and Telephone Acceptable Use Policy for School Staff

By signing this ICT and Telephone Acceptable Use Policy, I agree to the following:

- Any content I post online, including outside school time, or send in an email will be professional and responsible and maintain the reputation of the profession and school.
- Adhere to the Internet Acceptable Use Policy when using any online services and report any accidental access of material that contravenes it to the IT Manager or IT Technicians.
- Adhere to the Wireless Acceptable Use Policy when using the wireless system.
- To protect my own privacy I will only use a school email address and school telephone numbers as contact details for pupils and their parents.
- Not to use social media to communicate with students or parents and will reject invitations on those mediums. I will also reject requests from students to partake in social media, discussion forums, instant messaging and video messaging.
- Only use my personal mobile phone during non-contact time; during contact time it will be kept in silent mode and out of view, except in an emergency with the agreement of my line manager.
- Not use my personal mobile phone or other personal electronic equipment to photograph or video students or staff.
- Take all reasonable steps to ensure the safety and security of school ICT equipment that I take off site.
- Take all reasonable steps to ensure that all school issued devices are fully virus protected and not exposed to risks from virus infection.
- Support the school's approach to e-safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- Refer any safeguarding concerns I have to the e-safety lead or Safeguarding Officer.
- **Any school data stored on a mobile device, e.g. laptop, tablet computer or mobile phone with file storage capability or any removable media, including but not limited to 'memory sticks', SD cards and portable hard drives must be encrypted with a strong password.*[1]**
- **Accidental loss of sensitive data must be reported immediately to member of the Senior Leadership Team and the IT Manager.**
- **When finished using a computer you must log off or lock the computer before leaving. *[2]**
- **Computer, SIMS and email accounts must not be used by anyone other than the person they were issued to unless directed to do so by a member of IT Support – i.e. no sharing of accounts.**
- **Students may not use staff accounts at any time.**

- **Computer hardware, software and firmware may not be installed, upgraded or altered in any way without the explicit permission of IT Support.**
- **Report any IT related issues to IT Support without delay. This will help IT Support ensure the equipment is functional for all users to maximise teaching and learning.**

***1 – All issued mobile computer devices and removable storage mediums are encrypted. This encryption may not be removed or adjusted by anyone other than a member of IT Support under the direction of the IT Manager.**
***2 – If you are unsure how to lock a computer, please contact IT Support for help.**

By signing, I also understand:

1. That I have the same obligation to protect school data when working on a computer outside of school.
2. That the school may monitor or check my use of ICT equipment and electronic communications by manual and automated systems.
3. That by not following these rules I may be subject to the School's disciplinary procedures.

The School reserves the right to monitor telephone use, internet use, email and other material on its computer systems from time-to-time for various reasonable and necessary purposes including:

- Checking compliance with all regulations and policies
- Safeguarding
- Preventing or detecting crime
- Investigating or detecting unauthorised use
- Checking for viruses or other threats to the performance of the system
- Investigating abnormal system behaviour
- Resolving an issue
- Monitoring standards of service or training
- Maintaining or carrying out school business

Emails will not be read by anyone except the sender or recipient if they are clearly marked as such. However, this will not be the case where access to the content of the email is required for the prevention or detection of a suspected crime or to prevent the inappropriate use of email.

Investigations, other than day-to-day monitoring, require the authority of the Senior Leadership Team in order to take place and should be satisfied there are reasonable grounds for this request.

Personal Use:

THOMAS MORE CATHOLIC SCHOOL

The personal use of email or the Internet by staff is permitted providing that it is not excessive and does not interfere with the proper performance of that person's duties.

It is good practice to maintain a distinction between what is a school business email and what is a personal email, for example by marking personal emails as 'personal' and storing them in a separate folder.

Telephones, email and the internet must not be used to carry out private commercial activities.

Personal telephone calls should be kept as brief as possible. Permission will need to be sought from the Senior Leadership Team for any calls to premium or overseas numbers.

Read and understood by:

Print Name:……..

Signature:……

Date:……

Please retain this copy for future reference.

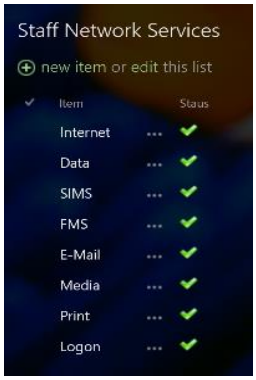
THOMAS MORE CATHOLIC SCHOOL

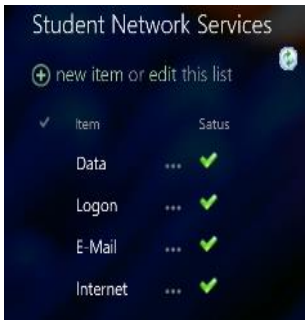
I.T. Support information:

Please note that there is a new email address for contacting I.T. Support / advising them of issues:

itsupport@tmore.org.uk

Before contacting I.T. Support, via any medium, do check the Intranet first for known issues. This is default Internet Explorer page for all users. Pay particular attention to these areas:





I.T. emergencies must be reported <u>verbally</u> by calling ext.218

Examples of emergencies include:

- A computer issue that directly prevents teaching and learning for a large number of students.
- Inability to access your email account to send an email.

Examples of requiring email only contact:

- *Requesting the computer and projector to be setup for assemblies.*
- *Faulty mouse or keyboard.*
- *Faulty computer, printer or interactive whiteboard.*
- *Faulty projector in classroom or hall.*
- *New content for TV displays in front entrance and website.*
- *Training for software packages or hardware.*
- *Viruses.*
- *Installing new software.*
- *Checking student use of computers during lessons.*
- *CCTV footage retrieval –* ***N.B. This requires email approval from the Head Teacher.***