I.C.T. ACCEPTABLE USAGE POLICY

School Name: **Ursuline Secondary School**

Address: **Templemore Road, Thurles, Co. Tipperary**

The B.O.M. & Staff at the Ursuline Secondary, Thurles believes in the educational value and opportunities offered by the schools I.T. facilities and recognise their potential to support the curriculum. Every effort will be made to provide quality experiences to students and teachers using these information services. However, inappropriate and/or illegal interaction with any information service is strictly prohibited.

The use of technology in Ursuline, should be in accordance with the ethos of the Ursuline. At no time is it acceptable to use any technology for the purposes of bullying, intimidation or hurting others.

School's Strategy

The school employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

General Guidelines

- The use of electronic services must be in accordance with the school's educational goals and objectives.
- All computer usage must be authorised and supervised by a teacher.
- Students are advised that using their own devices in school are governed by this policy. In addition, the unauthorised connection of personally owned devices to the school network is strictly prohibited.
- Filtering software is provided in conjunction with the school's broadband package supported by the NCTE, in order to minimise the risk of exposure to inappropriate material.
- Each student will be issued a unique Computer Network Account username and password. This will grant them access to the schools ICT resources at a student's security level. Students must use only their own username at all times (unless a specific account has been put in place for group work).
- Students and teachers will be provided with training in the area of Internet safety.
- The distribution of any information through the Internet/Intranet, social media platforms, email and any messaging systems through the school's network are subject to scrutiny by appropriate personnel.
- The use of all I.T. systems, resources and associated applications are subject to Irish and European law and any illegal use will be dealt with appropriately through the school disciplinary process.

- Users are asked to disconnect immediately, report and look for assistance if they access material or receive a message that is inappropriate. They should contact the Principal/Deputy Principal or any member of the I.T. Department.
- Uploading and downloading of any software (programs, images, music, videos any .exe files etc) is not permitted. If in any doubt a student should seek the teacher's permission before any such activity.
- Virus protection software will be used and updated on a regular basis.
- The use of personal devices, memory sticks or other digital storage media in school requires a teacher's permission.
- Printing facilities will be provided however permission must be sought from class teacher before printing any material
- Students are responsible for backing up their own work; the school; does not accept responsibility for any loss of material exam related or otherwise
- Students will observe good "netiquette" i.e. etiquette on the internet at all times and will not undertake any actions that may bring the school into disrepute.
- Students are not permitted to play games without the expressed permission of their teacher.
- Students may not enter a room with a computer(s) without an authorised member of staff being present.
- Food or drink is not allowed in the computer rooms.
- Students MUST log off their account when they have finished using a computer.
- Users may not bring into school an unmonitored internet connection (USB mobile plug in device etc), use any computer programs that have not been expressly permitted by the teacher or be logged into any instant messaging or social networking software while in school.

Personal Responsibilities:

As a representative of the school, each student must accept responsibility for reporting any misuse of the schools network to a staff member. Misuse may come in many forms, but it is commonly viewed as any messages sent or received that indicate or suggest pornography, unethical or illegal requests, racism, sexism, inappropriate language, any use which would be likely to incite hatred or which may be likely to cause offence and other issues described in this document.

Security & Monitoring:

- It is the school's policy that all students have a designated user account i.e. their own username and password assigned by the school
- Students are required to keep this information confidential as they alone are responsible for activity which takes place on their account. Students found disclosing passwords to friends or using another student's login information to gain access will be subject to disciplinary action
- If a student identifies a security problem she should notify a member of school staff immediately.

- Any user identified as a security risk may be denied access to the system and be subject to disciplinary action.
- The school reserves the ownership rights of individual student folders and as such may access these folders without seeking prior permission and may delete content if use is not in keeping with this policy.
- Data Storage: Where available, students should save their work files on the local server according to local practice, to ensure that it is backed up by the server.

Vandalism:

- Is defined as any malicious attempt to harm or destroy any equipment or data of another user or of any other networks that are connected to the system this includes but is not limited to the uploading or creation or computer viruses, the wilful damage of computer hardware, whether connected to the network or not, the deletion of data from its place of storage.
- Each student must report any damage to the class teacher at the beginning of class.
- Should students cause damage to the I.T. system, they are required to bear the cost of repairs/replacement.

World Wide Web:

- Students will not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Students will pupils report accidental accessing of inappropriate materials in accordance with school procedures.
- Students will use the Internet for educational purposes only.
- Students will not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).
- Students will never disclose or publicise personal information.
- Downloading materials or images not relevant to their studies, is in direct breach of the school's acceptable use policy.
- Students will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.
- Any student found deliberately trying to bypass the schools web filter will be subject to serious disciplinary procedures.
- I.T. facilities should not be used to make or post indecent remarks, proposals or any material which may bring the school into disrepute. Users are advised that any form of cyber abuse against the school/ another member of the school community is not tolerated. Any incidents of cyber abuse/bullying should be reported to the Deputy Principals/Principal and will be subject to disciplinary actions as set out by the Code of Behaviour.

Personal Safety:

- Students will not post personal contact information about himself or other people. Personal contact information includes address, telephone, school address, work address, photograph etc.
- Students will not agree to meet with someone contacted online.
- Students will not sign a 'guest book' on a Web page on behalf of Ursuline Secondary School.
- Students will promptly disclose to the Principal or the Deputy Principals, any message received that is inappropriate or which makes you feel uncomfortable.
- Students will not use artefacts associated with the school (e.g. the Ursuline Crest) on personal web spaces/pages.

Email:

- Students can only use email accounts under supervision by or permission from a teacher.
- Students will not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person.
- Students will note that sending and receiving email attachments is subject to permission from their teacher.

Internet Chat:

- Students will only have access to chat rooms, discussion forums, messaging or other forms of electronic communication that have been approved by the school.
- Where appropriate, usernames will be used to avoid disclosure of identity.
- Students may not create, access or sign guestbook's, message boards or bulletin boards.
- Students may not create, access or contribute to Web Logs (Blogging)
- The use of VoIP (Voice over IP) (for example, Skype) by students is prohibited

Online Ordering Systems:

- It is strictly forbidden for students of the Ursuline Secondary School, Thurles to use the internet for ordering goods or services online regardless of their nature.
- In addition it is also forbidden for students to subscribe to any newsletter, catalogue or other form of correspondence via the internet, regardless of its nature.

School Website - www.uct.ie

- The school website is controlled by the school authorities. It is not possible for pupils to upload information/data to this site. The publication of student work will be co-ordinated by a teacher.
- The school will endeavour to use digital photographs, audio or video clips focusing on group activities.
- Personal pupil information including home address and contact details will be omitted from school web pages.
- The school website will avoid publishing the first name and last name of individuals in a photograph.
- The school will ensure that the image files are appropriately named – will not use pupils' names in image file names or ALT tags if published on the web.
- Pupils will continue to own the copyright on any work published.

Personal Devices:

Pupils using their own technology in school, such as leaving a mobile phone turned on, sending nuisance text messages, or the unauthorized taking of images with a mobile phone camera, still or moving is in direct breach of the school's acceptable use policy.

Connecting or attempting to connect to the school's network system (wired or wireless) without authorisation is in direct breach of the school's AUP.

Mobile phones are strictly forbidden from 8.50 a.m. to 4.00 p.m.

Legislation:

The following pieces of legislation have relevance to internet safety:

- ***The Child Trafficking and Pornography Act, 1998***.
  This Act legislates against anyone who knowingly produces, prints, publishes, distributes, exports, imports, shows, possesses or sells child pornography.

- ***The Interception of Postal Packets and Telecommunications Messages Regulation Act, 1993***.
  This Act stipulates that telecommunication messages can be intercepted for the purpose of An investigation of a serious offence.

- ***The Video Recordings Act, 1989.***
  This prohibits the distribution of videos which contain obscene or indecent material which may lead to the depravation or corruption of the viewer.

- ***The Data Protection Act, 1988 and Amendment Act 2003***
  This Act was passed to deal with privacy issues arising from the increasing amount of information kept on computer about individuals.

Details of these acts can be obtained from:

http://www.oireachtas.ie/
http://www.irishstatutebook.ie
http://www.oasis.gov.ie/

Sanctions:

Misuse of the school computer facilities in accordance with the schools Code of Behaviour, sanctions may include verbal warnings, written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities. The use of the schools I.T. resources is a privilege and inappropriate use may result in that privilege being withdrawn.

Please read the above document carefully to ensure the conditions of use are accepted and understood. If you do not wish for your daughter to avail of the schools I.T. resources this must be addressed to the school principal in writing otherwise use will be granted as outlined.