POLICY DOCUMENT 53 – Approved 11/12/2017

Thomas Mills High School

ONLINE SAFETY POLICY

We, the staff and governors, aspire
to ensure that all our students,
irrespective of ability
and regardless of anyone's doubts,
achieve their potential in full;
and we aspire in this way to make Thomas Mills High School
the best in the country.

1. Curriculum

1.1. It follows from the Vision Statement above that the school views the provision of appropriate opportunities to use Information Technology (and to improve and increase ICT skills, knowledge and understanding) as a basic entitlement for all pupils.

1.2 All pupils must have opportunities for progression in the full range of ICT experiences. The ultimate aim is to help pupils to be confident in using ICT where it is relevant within any aspect of their work.

1.3 In order to ensure the basic entitlement at KS3 and KS4, ICT is taught as discrete lessons in Years 7, 8 and 9, supported by the inclusion in subject schemes of work. Computer Science is available as a GCSE option.

1.4 For many students post-16, opportunities to develop ICT skills will arise in their main courses, but to ensure opportunities for progress for other students. A level 3 technical award is offered alongside an A Level in Computer Science.

2. Acceptable Use by Pupils

2.1 Pupils are only able to gain access to the Internet and e-mail facilities in school by accepting the following guidelines:

- The School's connection to the Internet is provided as an additional resource for learning and all usage should be of an educational nature.

- Users must not search for, view or download material of an illegal, offensive or inappropriate nature. Any such material found by accident should be reported to a member of teaching staff or a member of the ICT department so that appropriate steps may be taken.

- Under no circumstances should social media sites be visited.

- Students should not accept or open any e-mail attachment if they are unsure of the name of the sender of the e-mail.

- Many items on the Internet are copyright and paper copies should not be made unless permitted. If in doubt, students should check with a member of staff.

- The opportunity to use the Internet and e-mail facilities is a privilege, given to assist students at their work.

- Students should be under no illusion. Any breach of these guidelines will have serious consequences for the user.

3. Particular Staff Responsibilities

3.1 Senior Management Team should:

- keep under review the use and suitability of the School's ICT facilities.
- revise this policy periodically for Governors' approval.
- ensure the provision of appropriate opportunities for INSET to support teachers in carrying out the School's policy.
- manage the School's website.

3.2 Senior ICT Manager should:

- exercise overall management of the ICT network and equipment renewal.
- manage the SIMS system.
- support the management of the School's website.
- manage ICT technical support staff.

3.3 Head of Information and Communication Technology should:

- provide specialist ICT courses to examination level.
- deliver specialist ICT classes to supplement the work in other subjects.

3.4 Heads of Department should:

- integrate ICT into their schemes of work.
- ensure that the ICT entitlement in the schemes of work is delivered to all teaching groups in each year.
- work with the Head of ICT to ensure that all teachers in the department are supported appropriately.

4. Safe Use of New Technologies:

4.1 This policy should be read in conjunction with the following policies:

- Data Protection Policy
- Management of Information Policy
- Safeguarding Policy
- Behaviour Policy

- Publication Scheme on Information Available under the Freedom of Information Act 2000.

4.2 The School's Mobile Phone Protocol is printed in the logbook. It includes the following:

- mobile phones must not be switched on in lessons
- in class, and in the Library, phones should not be in 'silent mode' or be used to receive or send text messages
- no photographs or video should be taken of anyone, staff or student, without the express permission of that person.

4.3 Advances in ICT software, hardware and applications develop rapidly. Protocols for Mobile Phones, Internet Access and email will normally be assumed to apply to other technology applications as they develop and are used by the school for example, Facebook and Twitter.

4.4 The Code of Conduct appended to the School's Safeguarding Children Policy includes the following:

> Adults are expected to keep personal and work e-mail addresses separate and to communicate electronically with students, including by text messaging if absolutely necessary via school mobiles, only on approved school business. If any exceptional circumstances arise these should be discussed with a Senior Manager beforehand.

4.5 The Behaviour Policy states:

> The school condemns the use of mobile phones, or 'cyber-bullying' by other electronic means, to cause hurt or suffering. Parents are advised, however, that there is necessarily a limit to what the school is able to do about such incidents when they happen outside school.

4.6 The ICT Curriculum is designed to be broad-based. It starts with an induction and computer safety course in Year 7. All Year 7 and 8 pupils follow National Curriculum guidelines during the discrete ICT lessons and these are supported by subjects incorporating ICT into their schemes of work. GCSE Computer Science is offered as an optional subject at KS4. Sixth Form students have the opportunity to study computer Science at A Level or an ICT Level 3 Technical Award.

4.7 Assembly and tutorial periods are used to remind pupils of safe ways of using the new technologies.

5. Procedures for Ensuring Security of Equipment and Data

5.1 The School is registered on the public Data Protection register.

5.2 There exists a detailed ICT Systems Emergency Recovery Plan (which is appended to this policy).

5.3 The Staff Handbook (B18) contains detailed information about what is available to staff in terms of facilities, equipment, Internet access, technical support etc.

5.4 All staff are expected to follow the guidelines below in order to protect data:

- Use all network passwords on a strictly individual basis. Do not share them with colleagues or pupils.

- Take steps to ensure that their password offers a good level of protection. (Passwords should be changed on a regular basis; should not consist of a single word but contain both text and numbers; should not be easily ‘guessable’, for example, a spouse’s name, child’s name etc;)
- Not allow pupils to use a computer which is logged on with their user ID. (Any files stored in the Staff Shared Area would then be accessible to the student. Files in this area include, for example, individual pupil assessment data, SEN register. To make these available would constitute an offence under the Data Protection Act.)
- Not allow pupils to log on to their laptop (as the ‘Briefcase’ is accessible to any user logged on the laptop).
- Not allow a pupil to use any PC that has access to SIMS.
- Not leave a PC/laptop logged on and unattended, particularly in the classroom, without ‘locking’ it.
- Take reasonable steps to keep laptops and mobile storage devices secure. (Do not leave such items lying around in the staff room or a classroom during weekends/holidays, nor leave them unattended on the back seat of a car, for example.)

5.5 Sensitive personal data should not be sent via e-mail (unless encrypted) or stored on mobile storage devices.

6. Disposal of Hardware or Electronic Equipment

6.1 Any redundant electronic equipment is disposed of via the Waste Recycling Centre at Foxhall Road in line with the Waste and Electronic Equipment (WEEE) Directive. It is stored securely on site beforehand.

6.2 Any redundant hard-drives or data tapes are physically destroyed.

APPENDIX 1

Thomas Mills High School
ICT Systems Emergency Recovery Plan

ICT Staff contact details:

		Ext. No.	External DD	Personal mobile (Only to be used in an Emergency)
Nick Jones	Senior ICT Manager	254	726676	Restricted access only
Jason Durrant	ICT Technician	252	726676	Restricted access only
Daniel Bell	Assistant ICT Technician	228		Restricted access only

Hardware Faults

All system critical equipment is covered by a hardware support contract. Curriculum servers and the MIS (SIMS) server have both Hardware and Software Support through Research Machines with ‘next day’ response for hardware failures. The vast majority of network switching gear is HP Procurve equipment and is covered by a lifetime guarantee.

Backup routine

All curriculum servers and the MIS server are backed up to a NAS device, located in a separate building, every weekday evening using Backup Exec software. Backups to tape are performed weekly. All backups are automatically verified within the backup procedure.

Backup logs are checked each morning to ensure the success of the previous evening backup. Regular test restore jobs are also carried out to ensure data can be successfully recovered.

A three week tape rotation is used on all servers with the most recent set of ‘Friday tapes’ being stored off site.

Server disc partition setup/allocation

Attached to this recovery plan is a sheet showing the setup of each server including IP address, subnet mask, backup device, Backup Exec version and serial number *.

Antivirus

All servers and network stations are covered by Symantec AntiVirus. Updates are downloaded daily and distributed to attached stations.

(* attached to copies held by ICT staff)

Appendix 2 – A copy of the Approved Use Policy which pupils' sign whenever they log on to the School system

School policy for the Educational Use of the Internet

- The School's connection to the Internet is provided as an additional resource for learning and all usage should be of an educational nature
- Users must not search for, view or download material of an illegal, offensive or inappropriate nature. Any such material found by accident should be reported to a member of teaching staff or a member of the ICT department so that the appropriate steps may be taken
- Under no circumstances should any chat room site be visited
- Users must not send e-mail communications that are nuisance mail or could be viewed as offensive
- Students should not accept or open any e-mail attachment if they are unsure of the name of the sender of the e-mail
- Many items on the Internet are copyright and paper copies should not be made unless permitted

INTERNET GAMING IS NOT ALLOWED DURING SCHOOL HOURS