



Policy on the Use of ICT and Electronic Devices

Note: This policy applies to all sections of the school including EYFS

1. ICT in the Curriculum

Technology has transformed the entire process of teaching and learning. It is a crucial component of every academic subject, and is also taught as a subject in its own right. All of our classrooms are equipped with projectors and computers and most with Interactive whiteboards. We have one ICT suite in the school and pupils may use the machines there and in the library for private study. We also have six class banks of laptops which the boys can use.

All of our pupils are taught how to research on the internet and to evaluate sources. They are educated into the importance of evaluating the intellectual integrity of different sites, and why some apparently authoritative sites need to be treated with caution, e.g. some free, on-line encyclopaedias do not evaluate or screen the material posted on them.

2. Technology in Pupils' Lives

Technology plays an enormously important part in the lives of all young people. Sophisticated games consoles, both static and portable tablets, together with Bluetooth, 3G, 4G and Wifi enabled mobile phones provide unlimited access to the internet, to SMS messages, to blogging (web logging) services (like Twitter), to Skype and Facetime (video calls, via web cameras built into computers, phones and tablets), to wikis (collaborative web pages), chat rooms social networking sites (such as Bebo, Facebook and MySpace) and video sharing sites (such as YouTube).

This communications revolution gives young people unrivalled opportunities. It also brings risks. It is an important part of our role at Thorpe House School to teach our pupils how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, bullying, harassment, grooming, stalking and abuse. They need to learn how to avoid the risk of exposing themselves to embarrassment in later life by posting material which they will subsequently regret. They also need to be educated and fully understand that any message they might send or anything they post on any website which is disrespectful, defamatory, offensive or misleading about either an individual or an organisation can lead to extremely serious consequences and possibly a criminal record.

3 The Role of the Head of ICT

With the vast range of technology available to young people, we recognise that blocking and barring sites is no longer adequate. We need to teach all of our pupils to understand why they need to behave responsibly if they are to protect themselves. This aspect is a role for our pastoral staff. The Head of ICT has a key role in maintaining a safe ICT learning environment at the school and in keeping up to date with the rapid succession of technical developments. He/she is responsible for the security of our hardware system, our data and for advising our teaching and administrative staff in the use of ICT. He/she monitors the use of the internet and pupil email accounts and will report inappropriate usage to the Headmaster, maintaining a log of incidents relating to internet safety in the school.

4 The Role of our Designated Senior Persons for Child Protection

We recognise that internet safety is a child protection and general safeguarding issue. Our Designated Safeguarding Lead has been trained in the safety issues involved with the misuse of the internet and other mobile electronic devices. He/she works closely with the Bucks Safeguarding Children Board (BSCB) and other agencies in promoting a culture of responsible use of technology, which is consistent with the ethos of the school. All of the staff with pastoral responsibilities are aware of e-safety issues. The school's comprehensive PSHEE programme covers e-safety, and in collaboration with the Head of PHSEE the DSL ensures that all year groups in the school are educated in the risks and the reasons why they need to behave responsibly online. All allegations of misuse of the internet which have Child Protection implications are brought to the attention of the DSL.

5 The Role of Parents

- 5.1 We seek to work closely with parents in promoting a culture of e-safety.
- 5.2 During school, teachers will guide pupils towards appropriate material. Outside school families bear the same responsibility for guidance as they exercise with other information sources such as television, telephones, films and radio.
- 5.3 We will always contact parents if we have any worries about their son's behaviour in this area, and we hope that they will feel able to share any worries with us. We recognise that not all parents may feel equipped to protect their son when they use electronic equipment at home. We therefore arrange information evenings for parents when an outside specialist advises about the potential hazards of new technologies, and the practical steps that parents can take to minimise the potential dangers to their sons without curbing their natural enthusiasm and curiosity.

6 Access to the School's ICT facilities

- 6.1 The school's ICT facilities cannot be accessed by any pupil until the boy concerned has logged onto the system using his public user name and private password. Once logged onto the system the school can enable an individual e-mail account for that pupil and offer him supervised access to the Internet. Before the school allows any pupil to use the internet, he must obtain parental permission. Both pupil and parents must sign and return the form which is Appendix 2 to this policy as evidence that approval having been given. The form also confirms that that the pupil will abide by the school rules on use of the Internet as listed in Appendix 1 and that his parents have read and agree to the content of this entire policy. When a boy logs onto the school system he has to renew on screen his agreement to abide by the rules of usage.

7 Use of Personal Electronic Equipment

- 7.1 We take the view that while a boy is at school there is no need for him to be in possession or use a mobile phone. We believe that boys should not be listening to music through headphones during the school day, but should be fully interacting with the people around them. There is also a danger that expensive items brought into school might be damaged or stolen. Therefore the following rules apply:

- All electronic items, including mobile phones, are banned from school.
- Boys who travel to and from school independently of their parents may bring their phones into school but they must be handed in at Reception on arrival and collected when leaving school premises at the end of the day.

- If any boy is found in possession of an electronic device, or is found using his phone without permission, then the device will be confiscated for a period of two weeks and the boy will also be given a major demerit.
- All electronic items brought into school are brought in at the owner's risk and the only protection for these is through a personal insurance policy.

7.2 If a boy uses any device, whether it is in school legitimately or otherwise, in a manner which is inconsiderate to those around him or for any form of cyberbullying (as determined by the Headmaster or Deputy Headmaster) then he will be punished in accordance with the Anti-Bullying and Behaviour, Discipline and Exclusions policies. More specifically it is forbidden to use cameras/video facilities on a mobile phone to photograph other members of the school community without their permission.

8 Cyberbullying

8.1 Cyberbullying is a particularly pernicious form of bullying, because it can be so pervasive and anonymous. There can be no safe haven for the victim, who can be targeted at any time or place. When pupils are using school ICT equipment they are generally supervised and the filters prevent inappropriate use. However, the school has no control over content sent from personal devices. Bullying and harassment in any form should always be reported to a member of staff. It is never the victim's fault, and he should not be afraid to come forward. The school should always be informed even if the cyberbullying is occurring outside school hours and off the premises.

9 Appropriate use of Technology

9.1 Communication

- We expect pupils to treat staff and each other online with the same standards of consideration and good manners as they would in the course of face to face contact.
- We expect a degree of formality in communications between staff and pupils, and would not normally expect them to communicate with each other by text, mobile phones or social media. There are exceptions to this and our policy on Educational Visits explains one set of circumstances when communication by mobile phone may be appropriate. Boys who come to school on the school bus might also legitimately be contacted on their mobile phone.

9.2 Keeping the School Network Safe

- Certain sites are blocked by our filtering system and our IT Department monitors pupils' use of the network.
- The ICT Department monitors email traffic and blocks SPAM and certain attachments.
- We give guidance on the reasons for always logging off and for keeping all passwords securely.
- Access to sites such as "Facebook" and similar social networking sites is not allowed on the school's network.
- We have strong anti-virus protection on our network, which is operated by the ICT Department.
- Any member of staff or pupil, who wishes to connect a removable device to the school's network, is asked to arrange in advance with the ICT Department to check it for viruses.

9.3 Promoting Safe Use of Technology

- Our guidance is that no one should put anything onto the web that they would not say to their grandmother!

- We offer guidance on the safe use of social networking sites and cyberbullying in PSHE lessons, which covers blocking and removing contacts from “buddy lists”.
- Our PSHE lessons include guidance on how pupils can identify the signs of a Cyber-stalker, or a groomer and what they should do if they are worried about being harassed or stalked online.
- We offer guidance on identity theft and keeping names, addresses, passwords, mobile phone numbers and other personal details safe. Privacy is essential in the e-world.
- We explain that any blog or photograph posted onto the internet is there permanently. Anything that has been deleted may be cached in a search engine, company server or internet archive and cause embarrassment years later.
- We give guidance on how to keep safe at home, by encrypting the home wireless network, not opening unknown attachments and reporting any illegal content. Similarly we cover how a mobile phone filter can be activated, and how to block nuisance callers.
- We advise on the responsible use of Skype.
- All pupils are encouraged to look after each other, and to report any concerns about the misuse of technology; or worrying issues to a member of the pastoral staff.
- The whole school takes part in an annual Cyber Awareness Week. Pupils of all ages are encouraged to make use of the excellent online resources that are available from sites such as:
 - Childnet International (www.childnet-int.org)
 - Digizen (www.digizen.org.uk) -
 - Cyber Mentors (www.cybermentors.org.uk)
 - Cyberbullying (www.cyberbullying.org)
 - E-Victims (www.e-victims.org)
 - Bullying UK (www.bullying.co.uk)

10 Misuse of Technology

- 10.1 We expect all pupils to adhere to this policy for the safe use of the internet and other associated technology. Copies are given to all pupils and their parents, and we may impose sanctions for the misuse, or attempted misuse of the internet, mobile phones and other electronic devices.
- 10.2 We will not tolerate any illegal material, and will always report illegal activity to the police and/or the Local Child Safeguarding Board (BCSB). If we discover that a child or young person is at risk as a consequence of online activity, we may seek assistance from the Child Exploitation and Online Protection Unit (CEOP).
- 10.3 If any pupil posts anything onto the Internet that could bring the reputation of the school or anyone associated with it into disrepute, either directly or by association, then that would also be regarded as a serious breach of school discipline and the Behaviour, Discipline and Exclusions policy would apply.
- 10.4 Although all of the following are covered by the general terms of this policy, for the purpose of clarification, it is forbidden to send or forward anonymous messages, spam, chain letters, prank messages, phishes, spoofs, ‘joe jobs’ and virals. All forms of cyber-beefing such as fraping are strictly forbidden. Posting anything on any website which is disrespectful, defamatory, offensive or misleading about either an individual or an organisation is forbidden.

11 Monitoring and review

- 11.1 The Headmaster monitors the effectiveness of this policy on a regular basis. He also reports to the Governing Body on implementation of the policy and on relevant changes that are necessary, caused by the advancement of the relevant technology.

11.2 The Governing Body reviews this policy annually or earlier if there are changes to the school's ICT provision.

June 2003

Review Date: April 2018

Reviewed October 2005
Reviewed: October 2007
Reviewed: February 2010
Reviewed: October 2010
Reviewed: February 2012
Reviewed: February 2013
Reviewed: February 2015
Reviewed: February 2016
Reviewed: October 2016
Reviewed: April 2017

Signed: _____ **Headmaster**

Signed _____ **Chairman of Governors**

Related Suite of Policies:

- Policy for Safeguarding and Welfare of Pupils
- Policy for Induction of New Staff in Child Protection
- Policy for Staff Interaction with Pupils
- Policy on Taking, Storing and Using Images of Children
- Policy on the use of ICT and Electronic Devices
- Procedures when Adults at school face allegations of abuse

APPENDIX I

Rules for Use of the Internet and E-Mail (as agreed by each individual pupil)

- a. In lesson time I shall use the school's ICT facilities as instructed by the teacher in charge of the lessons
- b. Outside lesson time I shall give priority to other computer users who need to use the ICT facilities in connection with school work, including internet and e-mail use.
- c. I shall never tell anyone my password, not even my best friend.
- d. I will not enter or use Internet chat rooms.
- e. I shall always tell a member of staff if I encounter anything rude, nasty or suggestive when I am using the school's computers. I shall not look for bad language or distasteful things while I am online and I shall not download or distribute any such material.
- f. I understand that anything which would be regarded as unacceptable if spoken aloud is equally unacceptable if typed onto a computer or electronic device and that I will be punished accordingly if I am found guilty of having done this.
- g. I shall only send e-mails to a person or organization outside of the school if I have asked for permission from a teacher.
- h. When I use the Internet or e-mail I shall never give my full name and address or telephone number to anybody or pretend to be anyone or anything I am not.
- i. I shall not pass on e-mail chain letters or send an unreasonable number of e-mails. I will only send e-mails with text messages unless I have been given specific permission by a member of staff to do otherwise.
- j. I know that my use of the Internet and e-mail will be monitored by a member of staff. I understand that I shall lose access to the Internet and my e-mail account if I do not follow these guidelines.
- k. I understand that I am not allowed to download and/or install any software from the Internet or any other source and that I must not open any attachments to e-mail unless instructed to do so by a member of staff.
- l. I will not download any web-pages.
- m. If work is brought in from home on a removable device the device must be checked for viruses by staff before the work can be accessed on the school's machines.
- n. I understand that information on the Internet may not always be reliable, that sources may need checking and that websites may be sponsored by advertisers.
- o. I am aware that the content of any website is protected by copyright and of the dangers of copyright infringement, e.g. when cutting and pasting articles and comments.
- p. Thorpe House's interpretation of these rules of use is final.

APPENDIX 2

Thorpe House School Internet and e-mail Permission Form

Please complete and return this form to the Headmaster's Office.

Pupil

As a school user of the Internet and e-mail, I agree to comply with the school rules on its use. I will use the network in a responsible way and observe all the restrictions explained to me by the school.

Pupil's Name : (Please print)

Form :

Pupil's Signature : Date :

Parent

As the parent or legal guardian of the pupil signing above, I grant permission for my son to use his school ICT login access e-mail and the Internet. I understand that pupils will be accountable for their own actions. I also understand that some material on the Internet may be objectionable and I accept responsibility for setting standards at home for my son to follow when selecting, sharing and exploring information and media.

I have read through the Thorpe House School Policy on the Use of ICT and Electronic Devices and fully endorse it.

Parent's Signature : Date: