E SAFETY POLICY

Drafted by:	Head of ICT	Approved by:	MJHS
Approval date:	November 2014	Next review date:	November 2015
ISI Policy Nos.:			

Introduction

a) This policy aims to:

   i. Equip children to deal with possible exposure to inappropriate content and contact via computers and the Internet.

   ii. Equip parents to help their children with eSafety.

   iii. Make staff aware of their responsibilities and how they can help children and parents in this area.

b) The scope of technology increases daily. We need to keep abreast of new developments and be aware that children may sometimes have greater knowledge than we do.

c) CEOP and Childnet publish resources which can be consulted where necessary.

d) The School reserves the right to monitor children's electronic communications and Internet use. Disciplinary action may be taken against any child found to have deliberately misused a computer in contravention of the School Rules.

e) This policy applies to the use of social media for both business and personal purposes, whether during working hours or otherwise. The policy applies regardless of whether the social media is accessed using our IT facilities and equipment or equipment belonging to members of staff or any other IT equipment.

Photographs

a) Photographs, audio and video recordings will, from time to time, be taken for assessments and record-keeping and may appear in School and marketing publications including magazines, prospectuses, websites and other digital formats, in line with the following guidelines:

   i. Only first names will be given for children whose photos are used in publicly-accessible media.

   ii. Where parents do not want their children's photos and names used in this way, they must inform the Head in writing.

iii. Full names will not be used without the parents' consent, except in the Mercury, Termtalk and in publicity material such as the winning teams, scholarships, etc. Where appropriate the School will seek explicit permission.

iv. Personal email addresses, postal addresses, phone or fax numbers will not be shown in conjunction with any photograph of a child.

v. The School will only use photographs of children who are suitably dressed, to reduce the risk of such images being used inappropriately.

b) Guidelines for Staff:

i. Photographs may only be used for school business.

ii. They must be stored on the School-provided ICT equipment (PCs, iPads, etc) and not on personal devices.

iii. No photographs or any other form of recording of a child may be shared on any website such as Facebook, Twitter, Flickr, etc, or any other publicly-accessible media except via the school's official channels

iv. Staff should be cautious when taking photographs where their intent might be misconstrued, and be aware of the sensitivity of such photographs.

Personal ICT Equipment

a) Children's personal laptops and other portable ICT equipment may be used only with the express permission of the Learning Support Unit.

b) The ICT Department must be consulted prior to any portable device being brought to School, to ensure compatibility and to set up any required software and resources (such as printers and network shares).

c) Inappropriate use may lead to confiscation. Parents will be informed at the earliest opportunity.

d) The School reserves the right to monitor the use of these resources for inappropriate use, and to take control of them (both physically and electronically) where necessary to enforce School rules and ensure appropriate behaviour.

Mobile Phones

a) Children may not bring to School their mobile phones or any other electronic devices (such as iPads and other "tablet" devices).

b) Staff may confiscate such devices and return them to parents at the earliest opportunity. They may not search any mobile device without either the child's or parents' consent.

c) Refer to the Boarding House policies for guidance on mobile phone use for boarders.

Children's Use of ICT

a) At the start of each term, the Head of ICT will reiterate the rules concerning safe use of ICT, and the potential risks of Internet access, including social media.

b) At the beginning of the School year, form teachers will ensure that children sign a form in their homework diary, which states:

i. I will only access the system with my own username and password, which I will keep secret.

ii. I will not attempt to access, modify or delete other people's files.

iii. I will use the computers only for school work during the school day.

iv. I will only e-mail people I know or people that a member of staff or parent has approved.

v. I will not attempt to bypass the school's access restrictions for Internet sites.

vi. The messages I send will be polite and responsible.

vii. I will not use the Internet for online chat unless directed to do so by a member of staff for teaching purposes.

viii. I will not give out my address or phone number on the website or in an e-mail.

ix. I will report to the head of ICT or my tutor, any unpleasant or inappropriate behaviour or messages sent to me.

x. I understand that the school may check my computer documents and monitor my Internet usage.

Social Media

a) Our policy is that Twitter, Facebook, MySpace, Tuenti, Beebo and similar websites are not allowed to be used by children except in specific eSafety lessons where privacy and safety issues are being discussed.

b) Guidance for Staff:

i. Do not accept "friend" requests from current pupils, and remember that ex-pupils may have friends or siblings still at the School.

ii. Ex-pupils who are "friended" should preferably be added to a friends list with appropriate privacy settings – e.g. preventing them from seeing all your photographs and groups.

iii. The service provider (e.g. Facebook) may change their privacy settings, which could inadvertently make public information you wanted to keep private. Be aware of these changes and regularly review your privacy settings.

iv. Assume that anything you post online could eventually make its way into the public domain. Consider the serious professional and personal consequences of careless posting.

v. If you need to set up an area on a social networking site for a school project, do not use your usual profile to do this – create one specifically for School use.

vi. If your friends and family post photographs online, be aware that you might be identified, either by chance or (for example) Facebook's facial recognition software "tagging" you automatically. You might want to

speak to friends and family to make them aware of the risks and ask them for their care and consideration.

vii. Seek approval from the Head/Bursar before they speak about or make any comments on behalf of the School on the internet or through any social networking site.

viii. Report to the Head/Bursar immediately if they see any information on the internet or on social networking sites that disparages or reflects poorly on the School;

Staff use of ICT

a) Equipment provided by the school is only to be used in line with your duties as an employee of the School. Information, programs and equipment may not be used for any other purpose.

b) You may not use School ICT equipment in a way (or for purposes) which might lead to increased risk of malware infection – such as accessing a file-sharing network or downloading illegal copies of programs.

c) If you encounter problems with your ICT equipment, you should report it to the Network Manager or Head of ICT as soon as possible.

d) All data you access should be treated as confidential. It is your responsibility to ensure it is safe by:

   i. Ensuring your password is sufficiently complex to defeat any "hacking" attempts.

   ii. Keeping your password secret and changing it regularly.

   iii. Changing your password immediately if you think anyone else might know what it is.

   iv. Informing the ICT Department if you suspect any unauthorised use of your network account, email or School ICT equipment.

   v. Making copies only of information you need for your job, and deleting such copies as soon as they are no longer needed.

   vi. Ensuring that any mobile devices on which you have configured your school e-mail account have, at a minimum, PIN lock, ideally they should be encrypted and protected with a password.

e) You may not install programs on your computer without the specific consent of the ICT Department. If you want to install software but lack sufficient privileges on your computer or the network, ask the ICT Department to install it for you.

f) Do not misuse the School email system, i.e. by sending defamatory, untrue, obscene, malicious or (in any other way) inappropriate messages. This may be considered gross misconduct and dealt with appropriately by the school.

g) If someone else gains unauthorised access to your email account, be aware that they might misuse it to your detriment. Inform the ICT Department immediately should you suspect such use.

h) The Teachers' Contract states:

i. The School has the right to monitor its telephone and computer systems that are made available to the Teacher and to monitor, intercept and record any communications made by the Teacher, including any type of telephone, e-mail or internet communications, for any purpose authorised under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and any amending or supplementary legislative or regulatory requirements and the Teacher expressly consents to the School doing so.

ii. The Teacher is prohibited from sending any email message which is, in the reasonable opinion of the School, abusive, obscene, defamatory, confidential, discriminatory or which may amount to harassment of another individual and the Teacher is prohibited from accessing or downloading from the Internet material which is illegal, pornographic, subversive, abusive or discriminatory. Failure to comply with this clause will be regarded as a serious disciplinary offence and may result in the dismissal of the Teacher.

i) If you receive an email which you believe was not meant for you, you should notify the sender immediately and delete the email as soon as possible.

j) If an email you receive is inappropriate (e.g. defamatory, containing a virus or is being used for attempted fraud, etc) you should notify the ICT Department immediately.

k) Never provide your personal contact details to children, including phone numbers, email addresses and personal blogs, websites or social media profiles. Only use School ICT to contact children, and only in line with your School responsibilities.

l) Do not use electronic communications to send messages to children except in line with your School responsibilities.

m) If you suspect a child is in crisis or at risk of harm, electronic communications should only be used as a last resort where other forms of communication are not possible. Use other means of contact and, where possible, ensure you do not act alone.