Ian Ramsey Church of England Academy
E-Security and E-Safety Agreement for all Staff and Pupils: Year 7 2016-2017

The school's ICT system is an excellent resource and offers great value to all staff and pupils. No security is 100% reliable however and accidents can happen. In order for it to be effective, to minimise the chances of unsavoury incidents, and reduce the opportunity for problems to occur, it has to be treated with respect and consideration. The rules listed below are to be followed for the good and safety of all pupils and staff at the school, and of those connected to the school through the local education authority's central network.

1) General

All E-Safety incidents, whether accidental or deliberate, will be logged and monitored by the E-Safety officer and Network Systems Manager. An incident is classified as any breach of the rules or policies in place to protect the staff and pupils or network.

No attempt should be made to bypass the school's filtering systems which protect users from viruses, crackers and inappropriate material. Any attempt to avoid using the firewalls will be dealt with as a serious incident that could potentially expose sensitive information to unauthorised persons.

All machines should be logged off after use. You should never use another person's account. You should never use another person's computer without their permission and them being present.

There should be no attempt to interfere with the hardware and cabling of the school system: this includes (but is not limited to) turning-off other pupil's computers and interfering with the keyboards, unplugging network connections and cabling.

2) Passwords and accounts

Pupils have passwords for log-on, internet and email. Each user is responsible for his/her password and computer account security. A single sign-on culture is promoted to allow the same username and password combination to access the computers, email system and virtual learning environment – it is essential, therefore, that passwords are sufficiently complex to keep people from guessing or 'brute forcing' your account.

These passwords must not be shared with any other pupil or member of staff. The ICT support team will NEVER ask you for your password via email, network messaging or the learning platform. Never respond to any request to send your password to anyone. If necessary we will ask in person but never electronically.

Pupils will be held responsible for access to systems and files under their passwords.

Passwords should not be easily guessable – effective passwords are made from: upper and lower-case letters; numbers and other alpha-numeric characters such as those printed on the numbers of a keyboard and accessed with a shift key.

Do not let other users watch you type in your passwords. Do not watch other users' type in their passwords.

Do not attempt to learn another pupil's password. Never share your password with another person.

The use of another pupil's password, or the use of a staff password, is a serious offence. This applies even if that person has "given their permission".

3) Storage Devices and downloading

Removable storage devices, such as memory sticks and mp3 players, are allowed, but only to access or save school-related work. No other files, including image and music files, should be downloaded or uploaded.

There should be no direct downloading from the internet without a teacher's permission.

Many viruses pose as legitimate files – these viruses can cause loss of data to you and other users. Never download an item unless you are sure of the content and that your anti-virus software is up to date and operating correctly.

It is essential that you keep home computers up to date with the latest operating system and antivirus patches and that you check your system and storage devices for viruses on a regular basis. The school holds no responsibility for loss of data on home systems due to the replication of viruses or Trojans onto removable storage devices.

It is your responsibility to ensure that data on removable devices does not contain information in breach of the 1984 Data protection act (or the 1998 revision). It is your responsibility to ensure safe transit and storage of your removable devices.

- -< - cut here- ->- -

4) Email Systems

All emailing should be conducted through the school's own email system or the county-provided staff email system. The use of 'anonymous Internet-based emailing systems' – i.e. accounts that we hold no information on – is forbidden to protect against all forms of cyber-bullying.

All emailing should be restricted to school use only. The system should not be used for informal social contact.

The use of email for abuse, threats, intimidation, slander or trouble-stirring is forbidden. Bad language or inappropriate content is also forbidden. All content will be filtered and users accept that their accounts may routinely be checked at random to ensure the safety and protection of children entrusted into our care.

5) Internet Access

The Internet should only be accessed during lesson times with the teacher's permission.

No attempt should be made to view specific websites containing images and/or text concerning violence, sex, bad language, abuse, racial or religious hatred – these include but are not limited to: Personal web/ blog /video sites (including social networking sites such as My Space, YouTube, Facebook and Piczo); game sites; fan sites; porn sites; cracking/hacking sites. The only exceptions are school-organised networking sites used for school purposed and directed by staff.

No attempt should be made to use the computer facilities for gambling, legal or illegal betting.

Whilst certain curriculum areas may utilise social networking platforms, E-Safety and E-security are paramount to our pupils and staff and we strongly encourage safe practices in using online applications that connect people together. You should never communicate with an unknown person and utilise sites that entice you to "talk to a stranger".

6) Other uses

No attempt should be made to access the files of other users, whether staff, pupils or outside bodies in an unauthorised manner.

No access to open access files, for example those in All Pupils, should be undertaken in class without the class teacher's implicit permission.

Inappropriate use of photos to make fun of or bully others is forbidden. The inappropriate digital manipulation of any photograph or video for similar activity is also forbidden.

Never introduce computer systems to the network that have not been authorised by the ICT support team. Doing so can cause the distribution of viruses and malware onto the ICT systems.

7) School Photography and Video Production

Staff and pupils are often engaged in curricular activities that are ideal for recording using photography or digital video to use in displays, school brochures and updating the website. These images and videos help prospective pupils and parents see the wide range of activities on offer at Ian Ramsey C of E School. If you prefer that your image is not used in any booklets, brochures and displays, or the school website please write to the school to inform us of your opt-out wishes and we will ensure your image is not used. By not responding directly you are agreeing to your image/child's image being used in such material.

8) Loan of equipment and Laptops for children

Equipment in the school is often loaned during the course of a day for lesson and coursework completion. All care should be taken with the items loaned. Larger, more expensive items will be checked for condition, signed out and in by the ICT support team. Any malicious damages to equipment will be chargeable and subject to discliplinary process.

9) Consequences to ignoring or breaching this agreement

These rules are not negotiable. Disobeying them can lead to sanctions ranging from removal of ICT access, detention and (depending on severity of the incident) ultimately, expulsion.

By not indicating otherwise your disagreement through written communication with the school, this document forms an agreement with you that there are policies and procedures in place to protect all using the systems at Ian Ramsey C of E School. It is not a direct right to access the ICT systems but a privilege given to all attending the school. The school has a right and a duty to protect all staff and pupils at Ian Ramsey and, by virtue to the fact we are connected to other schools on the Stockton Network, staff and pupils at other institutes also. Not accepting this agreement will lead to the removal of your access to ICT systems at the school in order to achieve this.

- - - - - - - < -< - cut here- ->- >- - - - - -

I hereby agree to the terms and conditions of the Ian Ramsey C of E Academy E-Safety and E-Security Agreement. I fully understand the implications of not following the guidelines set to ensure the safety of users and systems at the school.

Pupil Name: _____ **Tutor Group**:_____

(please print name)

Signed	-	**Signed**	**Date:**
(student)	-	(parent/guardian)	
	-		
_____	-	_____	

Please return this form to Mrs Cooney by xxxxxx September 2016