The Crypt School ICT Acceptable Use Policy

2017-2018

Lead Person : **Lead IT technician**
Governing Body Committee : **Property, Health & Safety**
Required by: **Legal requirement, DfE, Ofsted**

Rationale: to guide all students on what is appropriate and safe usage of IT in school. It also serves to support students in the understanding of safeguarding to protect themselves and others when working with IT in or out of school.

This policy is an extension of the School Rules, covering specifically the use of the Crypt School network and any computer equipment connected to it. For the purpose of this document an electronic, mobile, computing device (for example laptops, PC tablets, palm-tops and mobile phones) will be referred to as a PDA or portable digital assistant.

Section A - Computer Facilities

1. Overview

At the Crypt we allow all pupils access to our computer network, enabling them to use standard applications (word processing, spreadsheet, database etc.) as well as online facilities such as the Internet and electronic mail. Every pupil is issued with a username, password and an e-mail address at the start of their school career.

Access to the computer network is a considerable privilege and it is the pupils' responsibility to restrict themselves to usage which is ethical and appropriate. Failure to comply with the rules which govern the use of the network may result in either (a) punishment of the pupil, for example by means of the detention systems which operate at different levels in the school, or (b) removal of access privileges, or (c) in serious cases, reference to the pupil's Head of Year. Parents will be informed when serious breaches of the Acceptable Use Policy have occurred. Further action will be carried out if deemed necessary.

Pupils are encouraged to make use of ICT facilities in support of their studies in all subjects, including the writing up of coursework assignments and other projects. Recreational use of the network is also permitted, though within clearly stated limits which are designed to give priority to pupils wishing to use the computers for academic and other school-related work.

The school provides a network environment in which pupils can assume that their legitimate use of computers and the data that they store are secure against interference by other users. Pupils should not, however, assume that their activities are completely private. The school retains the right to determine appropriate use and to monitor user accounts and fileserver space as judged necessary. Hence, records of usage, files that have been stored, and e-mail messages that have been sent or received may be scrutinised by the members of staff responsible for management of the network either (a) during routine system maintenance, or (b) if there is reason to suspect misuse of the network.

The Crypt School makes no warranties of any kind, whether expressed or implied, for the service it is providing. The Crypt School will not be responsible for any damages, including the loss of data.

The Crypt School may update this AUP at any time and give notice that the policy has been updated via Email.

2. Rules

The following rules apply in all the areas of the school where computers are provided for access by pupils.

a. General Conduct and Use

- Pupils should conduct themselves in an orderly and quiet fashion, and must always show consideration for other users.
- No food or drink may be consumed.
- Any damage to computers, furniture or fitments should be reported to a member of staff without delay. The same applies to any apparent malfunction of equipment.
- Pupils using computers during lunch break and private study periods must leave the computer rooms in time to arrive punctually for their next timetabled commitment.
- Only one pupil should be seated and working at a computer at any one time.
- Chairs should be placed tidily in the rooms before leaving.
- Students should not take photos or video of other student or staff unless granted permission by a member of staff and consent of the person being photographed/recorded.
- Cameras on school IT equipment such as laptops or iPads can only be used with consent of a member of staff.
- All rules relating to behaviour (see behaviour policy) are also applicable in the online environment.

b. Use of the Network

- When logging on to the network, a pupil must always use his or her own user identification and password. Any attempt to impersonate another user will be treated as a serious offence, as will any attempt to interfere with data stored on the network by another user. These activities are in fact illegal under UK law.
- Never, under any circumstances, use another person's account or attempt to log on as a system administrator.
- Vandalism is defined as any malicious attempt to harm, modify, or destroy data of another user. The school network or other networks connected to the Internet must not be vandalised. This includes the uploading or creating of computer viruses.
- Harassment is defined as the persistent annoyance of another user, or interference with another user's work. Harassment must never occur; this includes, but is not limited to, the sending of unwanted email (see below).
- If you feel you can identify a security problem on the school system you must notify the IT technical team immediately. You must not demonstrate the problem to other users.
- Pupils must never divulge their passwords to other pupils or to users of computers outside the school. Any activity carried out under a login is the responsibility of that user. Any pupil who suspects that this has happened accidentally should change his or her password without delay.
- Before leaving a computer, pupils must always log off the network and check that the logging out procedure is complete.
- Pupils must not attempt to gain access to the local drive of any machine or to create local accounts (administrative or otherwise).
- It is strictly forbidden to attempt to share drives, folders or files across the network.
- Only software that has been provided on the network may be run on the computers. Pupils are not permitted to import or download applications or games. In many cases it is illegal to do so.
- Pupils must be aware of, and comply with, the restrictions placed on certain kinds of usage; notably the playing of games on particular machines and at particular times of the day, where others wish to do academic work.
- Memory Sticks must not be used by pupils to start and run MSN or other chat software, carry MP3 files or other Music files and software including games to be run or downloaded on the Crypt network.
- By logging onto the school network pupils are accepting the terms of this AUP

3. Wireless Network

The following rules apply in all the areas of the school where wireless access to the network is available.

- Pupils should not attempt to use the wireless network at school with any “unauthorized” devices which includes but not limited to PDAs and recreational or games machines.
- With the exception of school owned devices, such as the laptops, lower school students must get express permission from a member of staff and approval from the IT Technical team before they may use a wireless device to access the school network or the Internet. It must be demonstrated that without the access the pupil’s learning will be hindered.
- Sixth formers can bring personally owned devices in to get internet access via the BYOD network
- By connecting to the wireless network pupils explicitly agree to this AUP
- All the rules above in regard to using the network apply to using the network wirelessly.

Section B - Internet and E-mail

1. Overview

The school’s Internet access is via a service provided by EXA, a company that has been involved with IT in education for many years. The advantage of IFL is that it seeks to deny access to web sites known to contain offensive or inappropriate material. The IFL filter is continually updated, though there can be no absolute guarantee that unsuitable material is never available to users. Pupils are given training in effective use of the Internet as a research tool at various stages throughout their school career, such as Learning to Learn lessons at Key Stage 3.

We regard the use of the Internet to search for and use information related to a school subject or to a hobby as acceptable. Every pupil in the school has access to the Internet and has a school e-mail account.

2. Rules

E-mail and the Internet represent an important learning resource; however they can be wasted or abused. When using these facilities, pupils are expected to use their common sense and behave with normal standards of courtesy.

a. General Netiquette

Pupils must not:

- Send electronic communications which are impolite, indecent, abusive, discriminatory, racist or in any way intended to make the recipient feel uncomfortable.
- Disclose to a third party the personal details of any other pupil.
- Access any inappropriate Internet site.
- Breach another person’s copyright in any material.
- Upload or download any unauthorised software or attempt to run that software. In particular hacking, encryption and other system tools are expressly forbidden.
- Purchase goods or services via the computer network.
- Use the computer network to gain unauthorised access to any other computer network.
- Attempt to spread computer viruses.
- Engage in activities that are prohibited under UK Law. Thus the transmission of material subject to copyright or protected by trade secret is forbidden, as of course is any threatening or obscene matter

b. Personal Safety

In addition, pupils need to be aware that thoughtless use of e-mail and the Internet may jeopardise their personal safety either at school or outside school. Pupils should therefore:

- Never arrange a meeting in person with anyone they have “met” or only communicated with by computer, without prior parental approval.
- Not respond to messages or posts that are indecent, suggestive, belligerent, discriminatory, threatening, or which make the student feel uncomfortable or unsafe in any way. If such a message is encountered the pupil should report it to his or her form tutor and parents.
- Be aware that any person they “meet” or communicate with online may pretend to be someone else.

- Remember that anything they read online may not be accurate.
- Ignore offers that involve either financial transactions or personal meetings.
- Not disclose any personal details, such as their home address or telephone number, across the Internet.
- Not publish any other information which may be offensive to teachers or pupils.
- Understand that accessing extremist websites is strictly prohibited by both staff and pupils. Concerns arising will be passed to the safeguarding officer to follow up on. Filtering and monitoring software will be in place to try to block pupils from gaining access to any such sites.

c. Social Media or Collaborative Content

We recognizing that collaboration is essential to education, THE CRYPT SCHOOL may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users. Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally-identifying information online, or any other information which may be offensive to teachers or pupils even when posting out of school, as content cannot easily be removed once posted on to the internet. Inappropriate or offensive postings about other pupils, staff or the School will have serious consequences such as severe School penalty, police involvement or a criminal record. Students must abide by the rules of any social media platform that they use and should be mindful that any information posted publically is likely to remain in the public domain as it cannot be easily removed. This may have serious implications for future careers.

d. Mobile Devices Policy

THE CRYPT SCHOOL may provide users with mobile computers or other devices to promote learning both inside and outside of the classroom. Users should abide by the same acceptable use policies when using school devices off the school network as on the school network. Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Users should report any loss, damage, or malfunction to IT staff immediately. Users may be financially accountable for any damage resulting from negligence or misuse. Use of school-issued mobile devices, including use of the school network, may be monitored.

e. Personally-Owned Devices

Where students have been given permission by staff to use personally-owned devices they must only do so in a way that does not interfere with the delivery of instruction by a teacher or staff or creates a disturbance in the educational environment. Any misuse of personally-owned devices may result in disciplinary action. Therefore, proper netiquette and adherence to the acceptable use policy should always be used. In some cases, a separate network may be provided for personally-owned devices.

Written by Gordon Taylor – October 2012
Reviews by Gordon Taylor – ~~June~~ Nov 2017~~6~~
Approved by SLT – ~~May~~ Nov 2017~~4~~

Full Governors' Approved – ~~June~~ Dec 2017~~4~~
Next Review: ~~November~~ December 2018~~7~~