



The Crypt School ICT Acceptable Use Policy for Adults

2018-2019

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

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

1. This policy applies to all staff or property of The Crypt School and to those offered access to school resources. This document, which covers Internet, Intranet and e-mail use and which does not form part of the contract of employment, may be subject to amendment from time to time.
2. The Internet system (i.e. Internet, Intranet and e-mail) is the property of The Crypt School and may be subject to monitoring and access by the School at its discretion. All access to the internet and email system is automatically logged.
3. Use of the Internet system by school employees is permitted and encouraged where such use is suitable and is in accordance with the goals and objectives of the school. Abuse of such use may lead to disciplinary action being taken.
4. The Internet system is to be used in a manner that is consistent with the school's ethos, rules and regulations and as part of the normal execution of an employee's job responsibilities.
5. Generally, the Internet system should be used for business purposes. Reasonable personal use is permitted. However, users may be subject to limitations on their use of such resources.
6. The distribution of any information through the Internet system may be subject to the scrutiny of the school. The school reserves the right to determine the suitability of this information.
7. Users shall not:
 1. Visit Internet sites that contain obscene or other objectionable materials (not directly related to your area of work). The accessing or downloading of

pornographic material is prohibited and is likely to constitute gross misconduct, which may lead to dismissal.

2. Make or post indecent, demeaning or disruptive remarks, proposals or materials on the Internet system.
3. Copy, share, forward or display any material, whether internal or external, that is obscene or defamatory or which is intended or likely to harass or intimidate another person.
4. Disclose any information that is confidential, for example parents' personal details.
5. Represent personal opinions as those of the school.
6. Upload, download or otherwise transmit software or any copyrighted materials belonging to parties outside the school or to the school itself.
7. Download any software or electronic files without implementing virus protection measures that have been approved by the school.
8. Intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the network.
9. Examine, change or use another person's files, output, user name or password for which they do not have explicit authorisation. The use of computing resources is subject to UK law and any illegal use will be dealt with appropriately. The school retains the right to report any illegal violation to the appropriate authorities.
10. Leave laptop computers or any other easily transportable ICT equipment unattended at any time.
11. Ignore their duty of care for any of school ICT equipment in your possession, damaged equipment may not necessarily be replaced if there is a breach to the duty of care.
12. Damage to ICT equipment that is taken home. This should be claimed for under the home content insurance.
13. Use school Internet access for business, profit, advertising or political purposes is strictly forbidden.
14. Not take sensitive data off site unless it is encrypted. Data of individuals needs to be kept secure, especially when working with the School information System (CMIS/Eportal/Progresso) or any other personal data.
15. Do not reproduce copyright materials without first getting permission from the owner. Many people will make their work freely available for education on request. Acknowledge sources on all resources used.

Below are the rules for responsible internet and e-mail use which are published around the school. By logging onto the school's IT network, all adults are deemed to have explicitly agreed to the school's IT AUP and other school policies. Misuse of school's computer equipment, email or the Internet are serious offences. The Crypt School

Rules for Responsible Internet and E-Mail Use

At The Crypt School access to the computers and to the internet is a privilege. The school pcs and the internet are primarily used for learning. These rules will help us to be fair to others

and keep everyone safe. Failure to follow any of these rules will result in your access to the school network being restricted or denied.

- On the school network I will only use my personal username and password, which I will keep secret.
- I will not look at or delete other people's files.
- I will not bring floppy disks, cds or usb devices into school, without taking reasonable steps to ensure they are virus free
- I will only e-mail people I know, or that a member of staff has approved.
- The messages I send will be polite and sensible.
- When using e-mail or the internet, I will not give my full name, home address or phone number, or reveal the personal details of anyone else.
- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- I will not send any unsolicited promotional or advertising material nor any chain letters, pyramid selling schemes or virus warning letters.
- Make sure nothing in the messages could be interpreted as libellous.
- When using the Internet, Virtual Learning Environment or e-mail with pupils:
 - Remind pupils of the rules for using the Internet, cloud services or e-mail.
 - Watch for accidental access to inappropriate materials and report the offending site to the school's IT technical team and ask for the site to be blocked.
 - Check before publishing pupils' work on the school web site; make sure that you have parental permission.
 - Ensure pupils cannot be identified from photographs.
 - Report any breaches of the school's ICT AUP to your senior manager.

- I will not use Internet chat facilities social media sites or webmail (such as Facebook, Hotmail, Yahoo! Mail or AOL Mail) except during free time
- If I see anything on the internet I am unhappy or uncomfortable with, or if I receive messages I do not like, I will tell a member of staff immediately.
- 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 will be in place to try to block anyone from gaining access to any such sites.
- I know that the school may check my computer files and e-mails and may monitor the Internet sites I visit.

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful. Files and e-mails stored on the school network are property of the school not the user.

Full Governors' Approval: [July 2018]

Next Review: July 2019