THE KING'S SCHOOL
CHESTER

3.7 ICT and School Computer use

3.7.1 The following text is accessible from the front screen whenever a pupil logs into a networked computer. It is understood that all pupils agree to these rules. The statement detailed below applies to all computer and ICT usage within the School, whether on the network or on stand-alone machines. Compliance with the following laws is also agreed: The Computer Misuse Act 1990, The Criminal Justice & Public Order Act 1994, The Copyright Designs and Patents Act 1988, The Trade Marks Act 1994 and GDPR 2018.

When using the School computer network, I will:

- Access the network using my own username and password
- Keep my passwords secure and secret
- Not bring the School or myself into disrepute through my actions
- Perform only my School work
- Not visit offensive internet sites or chat sites
- Not use VPN's or other software to bypass school filters
- Not download files from the internet without permission from the IT Support Department
- Not load programs or change settings on the computers
- Not interfere with other users or their work
- Comply with all relevant laws and the school AUP

I understand that by clicking OK I agree to the above terms. My actions will be monitored and misuse may result in disciplinary action against me.

3.7.2 This policy applies to all computer and ICT usage within the School, whether on the network or on stand-alone machines.

3.7.3 Junior School pupils only use ICT and the school network under staff supervision. Junior School pupils are not allowed to carry mobile phones in school.

3.7.4 The policy is reviewed updated annually following discussion with pupil representatives and staff

3.7.5 Online safety is recognised as an important area of pupil education and impacts on all areas of teaching and personal development. As such the school aims to build knowledge, skills and capability. (see below Digital Technology Acceptable Use Policy: Pupil)

3.7.6 Staff must also be aware of their own online safety and responsibilities and the school ensures that staff receive appropriate online safety training that is relevant and regularly updated. [see Staff Technology Acceptable Use Policy and Staff Code of Conduct]

Summary of Staff Technology AUP

1. Policy statement
   The Governing Body has delegated day-to-day responsibility for the policy to the Head and the DFO. The IT support Department will deal with requests for permission or assistance under any provisions of this policy

2. The scope and purpose of the policy
   All staff are expected to comply with this policy at all times, failing to comply with this policy may result in disciplinary action which could result in a variety of sanctions, including dismissal

3. Equipment security and passwords
   Staff borrowing any equipment must comply with the device allocation and loan policies
   Passwords must be changed regularly to maintain security and ensure confidentiality
   School equipment should not be tampered with under any circumstances

4. Systems and data security
   No software should be downloaded onto the school network without consulting the IT Department
   No device should be attached to the school network without the prior approval of the IT Department ... this includes any USB flash drive, MP3 device, Phone, Laptop, Tablets or other Devices
   Any sensitive school data must be kept on Password Protected or Encrypted devices
   Confidential Information must be treated with extreme care and in accordance with GDPR

5. E-mail etiquette and content
   Correspondence sent by e-mail should be written as professionally as a letter or fax
   Staff should be aware of and avoid opening potentially damaging or insecure email attachments
   Staff should not send/resend chain mail, junk mail, cartoons, jokes or gossip, abusive, harassing, derogatory or defamatory e-mails

6. Personal use of systems
   We permit the incidental use of internet, e-mail and telephone systems to send personal e-mail, browse the internet and make personal telephone calls subject to certain conditions set out below:
   a. Use must be minimal and take place out of normal working hours
   b. Use must not extend to visiting inappropriate, illegal, immoral or offensive websites
   c. Use should not include the downloading or storage of any large or copyright protected files
   d. Use should not include the running of any games

7. Monitoring of use of systems
   School systems may enable us to monitor (and retrieve deleted) telephone, e-mail, voicemail, internet and other communications. Monitoring is only carried out to the extent management consider appropriate

8. Inappropriate use of equipment and systems
   Misuse, excessive use or abuse of the school telephone or e-mail system, or inappropriate use of the internet in breach of this policy will be dealt with under the school Disciplinary Procedure. Including:
   Pornographic, Criminal, Offensive or irresponsible conduct likely to bring the school or individual into disrepute
   false or defamatory comments regarding colleagues (including management)

9. Social Networking
   Staff should refrain from engaging with pupils and parents through any social network
   Staff should not conduct themselves in a way that is detrimental to the school, a colleague, pupils or parents

The Full Policy can be found on Firefly under Staff Policies, see link below:
https://firefly.kingschester.co.uk/whole-school/staff-policies

3.7.7 It is recognised that Online Safety is a significant area of risk for pupils as well as an area of opportunity. A proactive approach to online safety is taken through the Tutor programme in the senior school and through PSHE lessons (see 3.5 PSHE Policy) with reference to *UKCCIS Education for a connected world framework*. Content, Contact and Conduct are all areas of focus in line with KCSIE 2018 (Annex C)

DIGITAL TECHNOLOGY ACCEPTABLE USE POLICY: PUPIL

Introduction

As the use of the internet and other digital technologies becomes more widespread, for the protection of the school and the pupils it is necessary to set out guidelines. Pupils should read these guidelines carefully as failure to comply may lead to disciplinary action being taken.
The use of digital communication and information retrieval is no more than the addition of another medium and the same behavioural standards are expected of pupils as are the case with more traditional means of communication.

Digital media are constantly changing presenting new opportunities and challenges. These guidelines will be updated in light of experience and the technology itself.

Acceptable and unacceptable use of School ICT (hardwired and wireless)

ICT equipment and software are the property of the school and I understand that it is a criminal offence to use if for a purpose not permitted by its owner.

I understand that school ICT equipment must be used responsibly and I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
I will respect system security and I will not disclose any password or security information to anyone
I will not install any software or hardware.
I will not use VPNs or other software to bypass school filters.
I will ensure that all personal data is kept secure and is used appropriately.
I will respect copyright and intellectual property rights.
I will report any incidents of concern regarding e- safety to a member of staff.
I will ensure that any electronic communications with staff are appropriate and occur via an authorised school email address or via the schools Leaning Platform
I will not invite members of staff to be a 'friend' on any personal social networking pages and I will restrict public access to any information that I place on such sites if it compromises the position of the school.
I will adopt e-safety advice and develop a responsible attitude to system use and to the content I access or create.

The school may exercise its right to monitor the use of the school's technology, including data stored on the school network, internet access and email. The school will take the necessary action where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Acceptable and unacceptable use of personal digital devices

All students are asked to bring a browser to school in order to access web based educational content over the school WIFI network. All of the regulations in this policy apply to the use of such devices in school.

Furthermore, it is their responsibility to maintain the security of their device and to ensure that the school's wireless provision is not compromised. The school will not provide support for the device and will not be held responsible for its security.

Netiquette

The following general principles should be adopted:

- Remember the central values of the school: ambition, benevolence and cooperation.
- Think before you place any thoughts or images on the internet.
- Be polite. Do not send abusive, demeaning or belittling messages to others.
- Use appropriate language. Remember that you are a representative of the school and that you are using a non-private network.

As email is increasingly becoming the communication method used today, pupils may inevitably receive malicious messages at some point. Should you receive such communication via your school email account, please report it to the school so that the sender can be blocked and any required further action can be taken.

Other digital technologies

It is recognised that digital technologies have become an integral part of a student's life. The school is, however, primarily a place of work and as such students need to adhere to the following guidance.

Remove to Fifth year pupils are not permitted to carry mobile phones with them during the school day. The school day is considered to start at 8.00 am. Pupils should place any phone that they have brought to school in their lockers when they arrive in school and leave them there until 3.50pm. If you are found to have a phone in your possession, it will be confiscated and disciplinary action may follow. Sixth Form pupils are allowed to have phones in school, but these should not be used outside the classroom and then they should only be used to support learning. Sixth Form pupils can use their phones at any time within the Sixth Form Centre. After 3.50pm the academic school day has ended and pupils may use phones.

These devices should not be used for taking images of other pupils without the express permission of staff.

Tablets and other digital devices needed for lessons can be used in school. Students are responsible for the safekeeping and appropriate use of these devices. Students are encouraged to store these devices in their locked locker.

3G and 4G devices with mobile internet access should not be used to access any data or images which are blocked on the school network.

Specific disciplinary action may be taken against students who contravene these guidelines in accordance with the school's disciplinary procedures. This includes confiscation of devices and formal school sanctions.

Sending or requesting indecent images (Sexting) may be a pastoral issue but it may be a significant safeguarding issue. It is recognised that this behaviour can arise from an abusive relationship or it may be the result of misguided decision making. Once indecent or sexual images are released into the public domain it is very hard to retrieve the situation. For this reason, it is discussed fully with all pupils in SRE lessons. Where instances are brought to the attention of the School a full investigation will determine what level of referral is required.