King Edward VI High School

Headteacher Mr J Christey
West Way, Stafford. ST17 9YJ

Telephone: (01785) 258546 Website: www.kevi.org.uk
Email: headteacher@kevi.org.uk

KING EDWARD VI HIGH SCHOOL

ICT POLICY
(incorporating E-Safety)

Encouraging and supporting all our learners to "Be the best that they can be"

Approved Date **February 2017**

Head teacher

Mr J Christey

Governor

Mrs M Witts

Review Date **Every 3 years or as legislation changes**

Introduction

This policy will focus on all aspects of the use of ICT within King Edwards VI High School. This will include:

- Safe use the school ICT Network.
- Safer use of ICT facilities beyond the classroom school.
- Email and E-learning communication.
- Data exchange.
- Staff Laptop use and school related Data.
- Use teacher mobile devices.
- Use of ICT equipment belonging to staff and students utilised within the school.

Safe use of the school ICT Network

There are protocols in place to help ensure safe and responsible ICT use.

- The Acceptable Use Policy (AUP) is agreed to at every log onto the network for pupils and every 7 days or as and when changes are made for staff. This clearly states the user is entering a monitored site that will scan their activity looking for possible infringements relating to all aspects of possible abuse of the system.

- Use of the school network is monitored by Securus software.

- Staff activity is logged and scrutinised by the School Bursar.

- Student activity is logged and scrutinised by the Deputy Safeguarding Lead.

- Any infringements of the network logged by Securus are dealt with according to the Staff Discipline, Pupil Agreement and Safeguarding policy.

- User agreements are signed by staff and pupils on arrival at the school and kept on file for the duration of their stay.

- New staff receive information on the school's acceptable use policy as part of their induction.

- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.

E-Safety Awareness

- All Y7 students complete an 8 lesson course within their ICT lessons on E-Safety.
- All Y8 and Y9 complete a 3 lesson refresher on E safety at the start of the academic year.
- Y10 and Y11 have 3 assemblies per year on E Safety.
- As part of the VI Form induction all students have a E Safety refresher.
- E-Safety is re-enforced through the duration of the students' experience and is referred to throughout the students' ICT lessons with reference made in each year's schemes of work. This includes aspects of legislation prevalent to safe use and compliance of the law. This includes:
    - Copy right
    - Data Protection
    - Computer Misuse
    - Inappropriate Use
    - Cyber Bullying
    - Staying Safe
    - Child Protection.
- There is an area on the school website dedicated to E-safety that can be accessed by students and parents which is linked directly to the "Think U Know" Government website. This helps ensure all data is relevant and up to date.

Password, Data and PC Security

Password security is essential for staff, particularly as they are able to access and use pupil data.

Staff are expected to have secure passwords which are not shared with anyone.

The pupils are expected to keep their passwords secret and not to share with others, particularly their friends.

Staff and students are continuously reminded of the need for ensuring their PCs and data are kept secure. The following protocols have been implemented to try and eliminate possible breaches in security.

- School PCs automatically save all school data to a secure location which is Virus and Firewall protected, and backed up on a 24-hour cycle.
- Laptops are networked to the same secure drive.

Staff must not have any sensitive data that can reveal any personal data of both staff and students on their laptops or any removable media, unless this encrypted and password protected.

Staff are advised to use the terminal server if they are required to work on sensitive data when they are not in school. This ensures the data and communication of the data is kept within the protected environment of the school's system.

Staff and students must never access the network through any means other than their secure log-on. This, therefore, prohibits the use of anyone else's user accounts and passwords, hacking, cracking, or breaking of the school's security measures.

Managing the Internet

The internet is provided through Entrust's monitored and filtered connection providing over-reaching security. The school can access event logs for access, and also can impose its own filtering at a local level.

The following rules apply.

- Students will have supervised access to internet resources (where reasonable) through the school's fixed and mobile internet technology.
- All internet traffic is filtered and monitored through the schools dedicated server and software.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

- All users must observe copyright of materials from electronic resources.

- Any staff mobile devices connected to the school network are done via request to the ICT office and use the same settings that protect and monitor the school systems.

The internet filtering is set at varying levels dependent upon the user.

Restricted High

This restricts all internet access for non-verified users. (e.g. a user who has hacked into the system), or a student who has not had parental consent to access the internet when in school.

Restricted Moderate
This applies to key stage 3 and 4 students and non ICT staff including all teachers and admin.

ICT Staff
This is restricted to the ICT Admin Team.

Infrastructure

King Edward VI High School is aware of its responsibility when monitoring staff communication under current legislation and takes into account;

- Data Protection Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998.

Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.

The school does not allow pupils access to internet logs.

The school uses management control tools for controlling and monitoring workstations. (RM Manager, Securus, and Internet Logs.)

It is the responsibility of the school, by delegation to the Data Manager, to ensure that anti-virus protection and fire wall integrity is installed and maintained and kept up-to-date on all school machines, including laptops.

If there are any issues related to viruses or anti-virus software, the Data Manager should be informed.

Email

All email communication relating to staff, Governors and students must only go through the school Office 365 system. No other email accounts are to be used to conduct school related business.

It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced.

A school standard disclaimer is attached by default to all email correspondence.

Staff sending emails to parents or pupils are advised to ensure its content is checked thoroughly, and their line managers added to the Carbon Copy (CC) or Blind Carbon Copy (BCC).

The forwarding of non-school business related content is not permitted.

All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication.

Pupils must immediately tell a teacher/ trusted school based adult if they receive an offensive e-mail.

Staff must inform the Leadership Group Member responsible for ICT or Data Manager if they receive an offensive e-mail.

Staff should inform the Leadership Group Member responsible for ICT or Data Manager if they receive unsolicited junk or spam email.

Pupils are introduced to email as part of the ICT Scheme of Work in Y7, this is re-enforced in lessons at the start of the year in Y8 and Y9, and assemblies in Y10 through to Y13.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, gaming devices, smart phones, and wearable smart technology are familiar to children outside of school too. They often provide a collaborative, well-known device with internet access and thus open up risk and misuse associated with communication and internet use.

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

Staff may connect their personal mobile device to the school WIFI, for school use however this should be done through the ICT Data Manager. (Staff must be aware that the school's internet filtering and monitoring will then occur for traffic to their mobile device.)

VI Form students may connect their personal laptops to the school WIFI, however this must be done through the ICT Data Manager. (Students must be aware that the school's internet filtering and monitoring will then occur for traffic to their mobile device.)

Pupils are allowed to bring personal mobile devices/phones to school if they have written parental consent but must not use them in school at any time including break and lunch time. At all times the device must be switched off.

VI Form students may use their personal mobile devices/phones and Laptops within lessons at the discretion of the teacher.

The school is not responsible for the loss, damage or theft of any personal mobile device.

The sending of inappropriate text messages between any member of the school community is not allowed.

Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School provided Mobile devices

All of the above rules are applicable to school provided mobile devices.

Where the school provides mobile technologies such as phones, laptops and tablets for offsite visits and trips, only these devices should be used.

Where the school provides a laptop for staff, the member of staff must take full responsibility for its professional use and content. No inappropriate use of that device is allowed in or out of school.

The school may call in the laptop for periodic checks and maintenance. (SIMs upgrade, PAT Testing, new software etc.)

School use of Digital Images

Taking of Images and Filming

Digital images are easy to capture, reproduce and publish and, therefore, misuse. The school are aware that it is not always appropriate to take or store images of any member of the school community or members of the public, without first seeking consent and considering the appropriateness.

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment. This is recorded on SIMs for all staff members to access as and when appropriate. The vast majority of students do not mind images being used in school displays, publications or on the school website or Facebook and twitter accounts, however you must always check permission before publication.

Staff are not permitted to use mobile phones to record images of pupils, this includes when on field trips.

Staff should wherever possible use the school's digital equipment, and ensure that images are downloaded to only the school network. With the express permission of the Headteacher a personal digital camera may be used when appropriate, (where specialist equipment is needed, or where prolonged use of school equipment is not appropriate such as during a school residential) under

the conditions that images are down loaded only to the school network and not stored on any device or removable media.

Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record inappropriate or offensive images, or images of others that may be deemed as bullying or intimidating this includes when on field trips.

Staff and students must not distribute any images through digital or printed means that may breach copy right, break the law, or cause any member of the school community offense or embarrassment.

Publishing Pupil's Images and Work

On a child's entry to the school all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site Facebook and Twitter accounts
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends the school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting student work on the internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Storage of Images

Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks).

Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network.

When new images are imported into SIMS the previous image is automatically deleted by the system and replaced by the new one.

Webcams, CCTV and Video Conferencing

The school uses CCTV for security and safety of students, staff and visitors. CCTV notifications are displayed at the school entrance. For further information on the school's use of CCTV please refer to the CCTV Policy.

We do not use publicly accessible webcams or CCTV in school. Webcams in school will only ever be used for specific learning purposes as deemed appropriate as a learning resource and identified within schemes of work.

All pupils are supervised by a member of staff when video conferencing and the school keeps a record of video conferences, including date, time and participants.

Approval from the Headteacher is sought prior to all video conferences within school.

No part of any video conference is recorded in any medium without the written consent of those taking part.

Participants in conferences offered by 3rd party organisations may not be DBS checked.

Misuse and Infringements

Complaints

Complaints relating to King Edwards ICT use and facilities should be reported in line with the school's Complaints Policy, a copy of which is available on the school website. All incidents will be logged.

Inappropriate material (Staff)

Users are made aware of sanctions relating to the misuse or misconduct by the Acceptable Use Policy (AUP) and the ICT User Agreement, which is signed by the user and kept on file.

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Leadership Group Member responsible for ICT.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Leadership Group Member responsible for ICT, depending on the seriousness of the offence; investigation by the Headteacher/LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

Inappropriate material (Pupils)

Users are made aware of sanctions relating to the misuse or misconduct by the AUP which is displayed each time they log on to the network and a copy of which is included in the pupil planner, signed by the user.

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the teacher.

Deliberate access to inappropriate materials by any user will lead to the removal of Internet access/computer access as per Internet Access Removal procedure.

Equal Opportunities

Pupils with Additional Needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' e-Safety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned and well managed for these children and young people.

Parental Involvement

The school believes that it is essential for parents/carers to be fully involved with promoting E-Safety both in and outside of school. The school regularly consult and discuss e-Safety with parents/carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.

Parents/ carers are required to make a decision as to whether they consent to images of their child being taken or used in the public domain (e.g., on school website)

The school disseminates information to parents relating to e-Safety where appropriate in the form of;

- Information and celebration evenings
- Posters
- Website Facebook and Twitter postings
- Newsletter items

KING EDWARD VI HIGH SCHOOL

Current Legislation regarding the use of ICT in Schools

Data Protection Act 1998

The Data Protection Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individual's rights of access to their personal data, compensation and prevention of processing. For further information, follow the link below.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)

Interception of Communications Regulations 2000. For further information, please follow the link below.

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000 (RIP)

Regulating the Interception of Communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation. For further information, please follow the link below.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

For further information, please follow the link below.

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet). It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs. For more information, please follow the link below.

www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964 &
Criminal Justice and Licensing (Scotland) Act 2010: Section 42: Extreme Pornography

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.