KING EDWARD VI
HIGH SCHOOL

ADDRESS: Dryden Crescent, Stafford, ST17 9YJ
TEL: 01785 258546
WEB: www.kevi.org.uk
EMAIL: headteacher@kevi.org.uk
HEADTEACHER: Mr J Christey

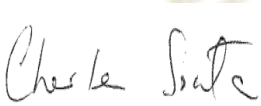
KING EDWARD VI HIGH SCHOOL

ICT & E SAFETY POLICY

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

Headteacher 

Mr J Christey



Governor

Mr C Soutar

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

WALTON
MULTI-ACADEMY TRUST

Ofsted
Good rating

Introduction

King Edward VI High School provides ICT facilities for use by its staff and students. These facilities come with responsibilities and this document summarises the standard of acceptable use that is expected from all staff and students using ICT facilities in 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 login onto the network, every 14 days or when content changes. 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.
- 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 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. Updates will be given on a regular basis

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.
- Staff must not have any sensitive data that can reveal any personal data of both staff or 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.

E-Safety rules

The following e-safety rules help to protect students when using the internet. These e-Safety Rules help to protect students and the school by describing acceptable and unacceptable computer use.

- It may be a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the Headteacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

- All network and internet usage is monitored including private encrypted traffic.

Acceptable Internet Usage

The following points are a guide to young people to be responsible and stay safe while using the Internet and other communication technologies. It clearly states what use of computer resources is acceptable and what is not. Irresponsible use may result in the loss of Internet or computer access, contact with parents or in the event of illegal activities contact with the police.

- I will only access the school network through my authorised username and password. I will not use the passwords of others.
- I will not use the school IT systems for personal or recreational use, for on-line gaming, gambling, internet shopping, and file sharing or video broadcasting.
- I will not try to upload, download or access any materials which are illegal, inappropriate or which may cause harm and distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place.
- I will not try to install programmes on any school computer or try to alter computer settings.
- I will only use my personal devices (e.g. mobile phone/tablet/laptop) in school at times that are permitted. When using my own devices, I understand that I have to follow the rules set out in this document and that I bring the device to school at my own risk.
- I will carefully write email and other on-line messages making sure the language I use is not strong, aggressive or inappropriate and shows respect for others. I am responsible for the emails I send and the contacts I make.
- I will not open emails unless I know and trust the person/organisation who has sent them.
- For my own safety and that of others, I will not disclose personal information about myself or others when online. I will not arrange to meet 'on-line friends' unless I take an adult.
- I will not take, or distribute, images of anyone without their permission.
- I will report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

- Where the material I research on the Internet is protected by copyright, I will not try to download copies, including music and video. I will only use the work of others found on the Internet in my own work with their permission.
- I will take care to check that information I find on the Internet is accurate and understand that some work found on the Internet can be untruthful or misleading.
- I will immediately report any damage or faults involving IT equipment, however this may have happened.

Managing the Internet

The Internet Service is provided by Contingency Networks Ltd and filtering is imposed at a local level using Smoothwall.

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.
- 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 the following 5 varying levels dependent upon the user.

<u>Restricted High</u>
This restricts all internet access for non-authenticated 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.

Key Stage 3 and Key Stage 4
Students in Years 7 through to 11

Key Stage 5
Students in Years 12 and 13

Non ICT Support Staff
Teachers and Support Staff other than ICT Support team

ICT Support Team
This is restricted to the ICT Support 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 2018
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Regulation of Investigatory Powers Act 2018
- 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 Smoothwall, Securus and Internet logs)

It is the responsibility of the school, by delegation to the ICT Technician, 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 ICT Technician should be informed.

Email

All email communication relating to staff, Governors, students and parents 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.

All messages which are sent from external accounts (outside of @kevi.org.uk), where addressed to student accounts are filtered and either approved or rejected by ICT staff, as appropriate

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.

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 Technician. (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 Technician. (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.

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

No image or sound recordings should 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.

For security purposes, the member of staff is responsible for ensuring that Windows updates and antivirus software is kept up to date by connecting the school network for updates.

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

School use of Digital Images

Linked policy – Photographs and Image Use Policy

Staff are not permitted to use mobile phones to record images of pupils, 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.

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

Linked policy – CCTV policy

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 Edward VI 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/Local Authority (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

Appendix 1

Current Legislation regarding the use of ICT in Schools

The Data Protection Act 2018

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.legislation.gov.uk/ukpga/2018/12/contents/enacted

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.

Appendix 2

Internet User Agreement and Parental Permission Form

Name: _____ Tutor Group: _____

User ID: _____

The following points are a guide to young people to be responsible and stay safe while using the Internet and other communication technologies. It clearly states what use of computer resources is acceptable and what is not. Irresponsible use may result in the loss of Internet or computer access, contact with parents or in the event of illegal activities contact with the police.

- I will only access the school network through my authorised username and password. I will not use the passwords of others.
- I will not use the school IT systems for personal or recreational use, for on-line gaming, gambling, internet shopping, and file sharing or video broadcasting.
- I will not try to upload, download or access any materials which are illegal, inappropriate or which may cause harm and distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place.
- I will not try to install programmes on any school computer or try to alter computer settings.
- I will only use my personal devices (e.g. mobile phone/tablet/laptop) in school at times that are permitted. When using my own devices, I understand that I have to follow the rules set out in this document and that I bring the device to school at my own risk.
- I will carefully write email and other on-line messages making sure the language I use is not strong, aggressive or inappropriate and shows respect for others. I am responsible for the emails I send and the contacts I make.
- I will not open emails unless I know and trust the person/organisation who has sent them.
- For my own safety and that of others, I will not disclose personal information about myself or others when online. I will not arrange to meet 'on-line friends' unless I take an adult.

- I will not take, or distribute, images of anyone without their permission.
- I will report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- Where the material I research on the Internet is protected by copyright, I will not try to download copies, including music and video. I will only use the work of others found on the Internet in my own work with their permission.
- I will take care to check that information I find on the Internet is accurate and understand that some work found on the Internet can be untruthful or misleading.
- I will immediately report any damage or faults involving IT equipment, however this may have happened.

Violations may result in loss of access as well as other disciplinary action. As a user of the King Edward VI High School computer network, I hereby agree to comply with the above stated rules and accept sole responsibility for the User ID which I have been given.

Student Signature _____ Date: ___/___/___

As the parent/guardian of the student signing above, I grant permission for my son/daughter to use electronic mail and the Internet. I understand that all students will be held accountable for their own actions. I understand that some material on the Internet may be objectionable and I accept responsibility for setting standards for my son/daughter to follow when selecting, sharing and exploring information media.

Appendix 3 Laptops for Teachers

We are pleased to offer you the use of this personal laptop. Please be aware that this device, and any additional accessories, remain the property of the school. Should you leave your employment with our school, the laptop and all additional accessories will need to be returned prior to leaving our employment.

It is your responsibility to:

- Ensure that the laptop and accessories are kept clean, in good working order and free from damage.
- Promptly report any damage and/or faults with the laptop or its accessories.
- Ensure your files and documents are stored securely. All work should be saved to your personal or shared network where they are securely stored and regularly backed up.
- Regularly update the laptops operating system and anti-virus software.
- Understand and comply with relevant ICT and Data legislation such as Computer Misuse Act, Copyright and GDPR.
- Understand and comply with all school ICT policies and network rules.

We strongly advise against the use of removeable storage devices. Wherever possible, files should be stored on our network or on school approved cloud storage, such as OneDrive or GoogleDrive. Should you choose to use any removeable storage devices, it is your responsibility to ensure they are adequately encrypted.

DECLARATION:

- I accept sole responsibility for the equipment issued to me as outlined above.
- I accept that I am to be the sole user of this equipment.
- I will ensure the laptop is always password protected.
- I am aware of my responsibilities with regard to the protection of data.
- I understand my responsibilities as a user of the school ICT network.
- I agree to comply with the school's ICT policies and rules.
- I will not use school equipment for any activity that is unlawful or illicit.
- I understand that any suspected or actual computer virus infection must be reported immediately to the System Administrator.

Appliance ID	Make	Model	Serial Number

Name		Date

Appendix 4

Acceptable Use Agreement for Staff

We are pleased to offer you the use of our school network as well as other available ICT systems, such as email. Before access is granted, you are required to read and agree to following the schools Acceptable Use Policy as summarised below.

Declaration:

All users have a responsibility to support and encourage the security of all ICT resources and as an authorised user of King Edward VI High School's school network and ICT systems I confirm that:

I have read, understood and accepted all rules identified in the school's ICT and E-Safety Policy.

I will only access the ICT system(s) with the account(s) that I have been authorised to use.

I will not exceed any access rights granted to me by the system manager.

I will ensure I lock or log out of any active connections to the school's ICT systems so as to prevent unauthorised access by others.

I understand, and will adhere to, my responsibilities in regard to current legislation;

- General Data Protection Act (GDPR)
- Data Protection Act 2018
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Telecommunications Act 1984

I understand that any infringement of this legislation, relating to the use of ICT systems, may result in loss of access, disciplinary, civil and/or criminal action against me and/or the school.

I will not use school equipment to access, send or display inappropriate material such as pornographic, racist or that which may be deemed offensive.

I will report any suspected or actual computer virus infection immediately to the system manager, including any interaction(s) with emails that may be SPAM.

I will pay due regard to the sensitivity and confidentiality of any information I am granted access to.

Name		Date
Signature		