KING EDWARD VI SCHOOL
SHAKESPEARE'S SCHOOL

IT Acceptable Use Policy

Reviewed 18.11.25

Overview

The intention for publishing an IT Acceptable Use Policy is not to impose restrictions that are contrary to the School's established culture of openness, trust and integrity. The School seeks to protect its staff, students, and the Governing Body from illegal or damaging actions by individuals, either knowingly or unknowingly.

The School network related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and FTP are the property of the School. These systems are to be used primarily for School related purposes in the course of normal day-to-day activities. The use of network related facilities is permitted for occasional personal use, for example, non-school related use of email and the World Wide Web, but these activities are also subject to this acceptable use policy. It is the responsibility of every user to be familiar with these guidelines, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment, smartphones and tablets at the School. These rules are in place to protect the users and the School. Inappropriate use exposes the School to risks including virus attacks, compromise of network systems and services, and legal issues. All School-owned network systems—including computers, software, storage, email, and internet access—are the property of the School and must be used primarily for educational and administrative purposes. Occasional personal use is permitted but remains subject to this policy.

Scope

This policy outlines acceptable use of School-owned computer equipment, smartphones, tablets, and personal devices connected to the School network. It aims to protect users and the School from risks such as malware, data breaches, and legal issues.
This policy applies to staff, students, contractors, and visitors using the School network.

Policy

General Use and Ownership

1. While the School desires to provide a reasonable level of privacy, users should be aware that the data they create on the School systems remains the property of the School. Because of the need to protect the network assets, the confidentiality of information stored on any network device belonging to the School cannot be guaranteed.
2. Users are responsible for exercising good judgment regarding the reasonableness of personal use, if there is any uncertainty, users should consult the Network Manager.
3. For security and network maintenance purposes, authorised individuals within the School may monitor equipment, systems and network traffic at any time.
4. Students must check their personal device daily to ensure the device is charged, free from unsuitable material and free from viruses, before bringing the device into School
5. Students must check their personal device daily for basic Health & Safety compliance to ensure it is free from defects.
6. Students must not bring into School, or use, privately owned chargers for personal devices.
7. The School reserves the right to inspect and check any device if there is a reason to believe that a user has violated School policy or has engaged in other misconduct whilst using the device.

Security and Proprietary Information

1. All student and staff details, including photographs, are considered to be confidential and should not be disclosed to third parties, without the prior agreement of the Headmaster.
2. Users must only log on using their own user name and password. They are responsible for keeping their passwords secure/changed regularly and for logging-off when leaving a computer unattended.
3. Users are responsible for all activity carried out under their username. Without proof, claims that a password has been stolen will not be accepted as an excuse if unacceptable use is found to have taken place on a particular account.
4. Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, if in doubt seek the advice of the Network Manager.
5. Confidential information, including printouts, must be secured against unauthorised viewing (e.g. in a locked room or cabinet) and properly disposed of when no longer needed, following secure shredding practices.

6. All network users must set a compliant password of at least 8 characters containing a capital letter and a number or special character, and this password must not include the user's name or a part of their name. Users are also required to configure Multi-Factor Authentication (MFA) on first use of their account, using either the Microsoft Authenticator App, or via a text code or phone call. Passwords expire every 90 days.

Unacceptable Use of the IT Network

Under no circumstances is a user authorised to engage in any activity that is illegal under national or international law while utilising School owned resources. The list below is by no means exhaustive, but attempts to provide a framework for activities that fall into the category of unacceptable use. The following activities are **strictly prohibited**, with **NO** exceptions unless stated otherwise:

1. Online activity, both in and outside School, that will cause others distress or bring the School into disrepute.
2. Using the School computing assets to actively engage in the viewing, creation or distribution of any sounds, messages or other material which are obscene, harassing, racist, extremist, inflammatory, malicious, fraudulent or libellous, and which would otherwise damage the reputation of the School. If a user accidentally comes across any such material they must report it immediately to the Network Manager.
3. Unauthorised copying of copyrighted material including digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the School or the end user does not have an active licence is strictly prohibited.
4. Introduction of programs into the network or server without permission of the Network Manager
5. Allowing use of your account by others.
6. Accessing, or attempting to access data of which the user is not an intended recipient or logging into another account that the user is not expressly authorised to access. Circumventing user authentication or security of any work-station or user account.
7. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, the work of others, or result in the person receiving them losing their work or system access.
8. Providing information about, or lists of, users to parties outside the School.
9. Using the School systems for personal financial gain, gambling, political activity, advertising or illegal purposes.
10. Sending anonymous messages or chain mail with only exception being the use of Share.

11. Arranging to meet someone over the internet unless this is part of a School project approved by a member of staff.
12. Sending unsolicited messages, regarding the School to individuals who did not specifically request such material.
13. Any form of harassment via email, messaging, telephone, text or paging, whether through language, frequency, or size of messages. Solicitation of email for any other email address with the intent to harass or to collect replies.
14. Unauthorised use, or forging, of email header information.

Users must inform the Network Manager immediately if they receive an email through the School email system that they believe advertises a website containing indecent images of children.

Remote Access Requirements

Users must only access the School network and data using approved methods, such as the School's Virtual Private Network (VPN) or sanctioned web portals, using their assigned username and password. Multi-Factor Authentication (MFA), as configured under the "Security and Proprietary Information" section, must be used for all remote access where applicable.

Users are responsible for the security of their remote working environment. This includes ensuring their home or public Wi-Fi network is password-protected and that sensitive information is not viewed or discussed in a way that can be overheard or seen by others.

Student Conduct

1. Students must immediately inform a member of staff if they receive an offensive electronic communication.
2. Students must not reveal personal details of themselves or others in electronic communication or arrange to meet anyone without specific permission.
3. Student to staff electronic communication must only take place via a School email address or Microsoft Teams and will be monitored.
4. Incoming email must be treated as suspicious and attachments not opened unless the author is known.
5. Students must seek authorisation for any email sent to external bodies when representing the School.
6. Students will be advised never to give out personal details of any kind which may identify them or their location. They are advised to use nicknames and avatars when using social networking sites.
7. Students must not place personal photos or videos on the network without permission.

Social Networking

1. Students and parent will be advised of risks associated with social networking.
2. Student must never share identifying personal details.
3. Students are encouraged to use nicknames and avatars when social networking platforms.
4. Do not upload personal photos or videos without permission.

Reporting Incidents

Any suspected security breach, theft, loss of a device, or compromise of confidential data occurring during remote work must be reported to the Network Manager immediately.

Policy Review

This policy will be reviewed annually, or sooner if significant changes occur in technology, legislation or School requirements.The review will be conducted by the Network Manager in consultation with the School Business Manager and approved by the Governing Body. The next scheduled review is November 2026.