KPA Acceptable Use Policy

1 Overview

The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources at King’s Preparatory Academy in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.

King’s Preparatory Academy provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This policy requires the users of information assets to comply with company policies and protects the company against damaging legal issues.

2 Scope

All employees, contractors, consultants, temporary and other workers at King’s Preparatory Academy, including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned or leased by King’s Preparatory Academy, or to devices that connect to a King’s Preparatory Academy network or reside at a King’s Preparatory Academy site.

Information Security must approve exceptions to this policy in advance through the Office of Student Services.

3 Policy Statement

3.1 General Requirements

3.1.1 You are responsible for exercising good judgment regarding appropriate use of King’s Preparatory Academy resources in accordance with King’s Preparatory Academy policies, standards, and guidelines. King’s Preparatory Academy resources may not be used for any unlawful or prohibited purpose.

3.1.2 For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic per the Audit Policy. Devices that interfere with other devices or users on the King’s Preparatory Academy network may be disconnected. Information Security prohibits actively blocking authorized audit scans. Firewalls and other blocking technologies must permit access to the scan sources.

3.2 System Accounts

3.2.1 You are responsible for the security of data, accounts, and systems under your control. Keep passwords secure and do not share account or password information with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.

3.2.2 You must maintain system-level and user-level passwords in accordance with the Password Policy.

3.2.3 You must ensure through legal or technical means that proprietary information remains within the control of King’s Preparatory Academy at all times. Conducting King’s Preparatory Academy business that results in the storage of proprietary information on personal or non- King’s Preparatory Academy controlled environments, including devices maintained by a third party with whom King’s Preparatory Academy does not have a contractual agreement, is prohibited. This specifically prohibits the use of an e-mail account that is not provided by King’s Preparatory Academy, or its customer and partners, for company business.

3.3 Computing Assets

3.3.1 You are responsible for ensuring the protection of assigned King’s Preparatory Academy assets that includes the use of computer cable locks and other security devices. Laptops left at King’s Preparatory Academy overnight must be properly secured or placed in a locked drawer or cabinet. Promptly report any theft of King’s Preparatory Academy assets to the Office of the Dean.

3.3.2 All PCs, PDAs, laptops, and workstations must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

3.3.3 Devices that connect to the King’s Preparatory Academy network must comply with the Minimum Access Policy.

3.3.4 Do not interfere with corporate device management or security system software, including, but not limited to, antivirus, Google or Google Docs sites, Planning Center, Infinite Campus or any other web-based applications, Norton Anti-Virus or Select Block systems for security or device management.

3.4 Network Use

You are responsible for the security and appropriate use of King’s Preparatory Academy network resources under your control. Using King’s Preparatory Academy resources for the following is strictly prohibited:

3.4.1 Causing a security breach to either King’s Preparatory Academy or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device; or sniffing network traffic.

3.4.2 Causing a disruption of service to either King’s Preparatory Academy or other network resources, including, but not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.

3.4.3 Introducing honeypots, honeynets, or similar technology on the King’s Preparatory Academy network.

3.4.4 Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software. See the Acceptable Use Addendum on Additional Restrictions for additional information on copyright restrictions.

3.4.5 Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws. See the Acceptable Use Addendum on Additional Restrictions for additional information on export and transfer restrictions.

3.4.6 Use of the Internet or King’s Preparatory Academy network that violates the Acceptable Use Policy, King’s Preparatory Academy policies, or local laws.

3.4.7 Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and keyloggers.

3.4.8 Port scanning or security scanning on a production network unless authorized in advance by Information Security.

3.5 Electronic Communications

The following are strictly prohibited:

3.5.1 Inappropriate use of communication vehicles and equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates King’s Preparatory Academy policies against harassment or the safeguarding of confidential or proprietary information.

3.5.2 Sending Spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication.

3.5.3 Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.

3.5.4 Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

3.5.5 Use of a King’s Preparatory Academy e-mail or IP address to engage in conduct that violates King’s Preparatory Academy King’s Preparatory Academy policies or guidelines. Posting to a public newsgroup, bulletin board, or listserv with a King’s Preparatory Academy e-mail or IP address represents King’s Preparatory Academy to the public; therefore, you must exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the company.

4 Enforcement

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with King’s Preparatory Academy.

5 Definitions

Term	Definition
honeypot, honeynet	Network decoys that serve to distract attackers from valuable machines on a network. The decoys provide an early warning for intrusion detection and detailed information on vulnerabilities.
Spam	Electronic junk mail or junk newsgroup postings. Messages that are unsolicited, unwanted, and irrelevant.

6 Revision History

Date of Change	Responsible	Summary of Change
26 June 2017	Lisa Noel Babbage	Policy created