The King's School
Canterbury

VATTANACVILLE

Cyber Safety Policy

Reviewed: May 2024
Review Frequency: 2 years
Next Review: May 2026
Governor sign off: Yes/No

Contents

1. Introduction And Aim

In today's digital age, the safety and security of our digital environment are paramount to the well-being of our school community. The King's School Vattanacville is dedicated to ensuring that all members of our community, including staff, governors, volunteers, contractors, parents, and pupils, are protected from cyber threats and misuse of digital resources.

With the increasing reliance on technology for educational and administrative purposes, it is essential to establish clear guidelines and procedures to safeguard our digital infrastructure. This policy aims to foster a culture of cyber safety, promote responsible use of technology, and provide a secure environment for teaching, learning, and administration.

Cyber safety involves proactive measures to protect against unauthorized access, cyberbullying, online fraud, and other digital threats. It also includes educating our community about best practices for safe internet use and ensuring that our digital resources are used ethically and responsibly.

This Cyber Safety Policy outlines our commitment to maintaining a secure digital environment and provides a framework for preventing, detecting, and responding to cyber incidents. By adhering to this policy, we aim to protect the integrity, confidentiality, and availability of our digital resources and support a positive digital experience for all members of The King's School Vattanacville.

2. Purpose Of the Cyber Safety Policy

The Cyber Safety Policy applies to all staff at the King’s School Vattanacville and has the following aims:

- Protect the school's digital infrastructure and data for staff, parents, and pupils.
- Safeguard the personal information and digital assets of staff, parents, and pupils.
- Educate and inform the school community about cyber safety and best practices.
- Establish clear procedures for handling cyber incidents and breaches.

In fulfilling our duty to protect the digital infrastructure and data of The King's School Vattanacville, we also recognize the importance of safeguarding the personal information and digital assets of our governors, staff, parents, and pupils. Cyber threats can target individuals at all levels of the school community, and it is our responsibility to ensure that everyone is equipped with the knowledge and tools to mitigate these risks.

This policy aims to create a safe and secure digital environment for staff, parents, and pupils by:

- Implementing robust security measures to protect against cyber threats.
- Providing regular cyber safety training and resources to educate the school community.
- Establishing clear guidelines for acceptable use of digital resources.
- Ensuring prompt and effective response to cyber incidents to minimize impact and prevent future occurrences.

By adhering to this policy, we are committed to protecting the integrity, confidentiality, and availability of our digital resources, as well as the privacy and safety of our staff, parents, and pupils.

3. The Policy Scope

This policy applies to all governors, staff, volunteers, contractors, parents, and pupils of The King's School Vattanacville who use the school's digital resources or access the school's network. It covers all devices owned or provided by the school, including but not limited to computers, laptops, tablets, smartphones, and other electronic devices.

The policy applies to all digital activities conducted on school premises, as well as off-site activities that involve the use of school digital resources. This includes, but is not limited to, accessing the school's network, using school-provided email accounts, accessing school databases or online platforms, and using school-owned software or applications.

Personal moveable devices will be exclusive to the Quest network. And all accepted letters will have to be signed before connecting to the school ICT facilities.

The finance sector is often a prime target for cyberattacks, as threat actors recognize the potential financial gains. This is especially true in the context of the game 'Hacked for the Money', where players simulate such attacks to understand the challenges faced by financial institutions.

4. The Policy Definitions

To identify and understand the target of a threat for specific purposes, we need to know about:

- **Cyber Safety:** The practice of protecting information systems, networks, and data from cyber threats, including but not limited to hacking, phishing, malware, and other malicious activities. Most of the security issue and leakages in Cambodia are via Telegram. Except for use by personal phone and the Admissions and Marketing Team, Telegram should not be used on school devices.

- **Digital Resources:** Any hardware, software, data, or information systems provided or used by The King's School Vattanacville, including but not limited to computers, laptops, tablets, smartphones, servers, networks, and online platforms.
- **Cyber Incident:** Any event or occurrence that poses a threat to the confidentiality, integrity, or availability of digital resources, including but not limited to unauthorized access, data breaches, and malware infections.
- **Personal Information:** Any information that identifies or can be used to identify an individual, including but not limited to names, addresses, phone numbers, email addresses, and identification numbers.
- **Sensitive Data:** Information that requires special protection due to its sensitive nature, including but not limited to financial information, health records, government-issued identification numbers, and other confidential information. Pupils and parent information records.
- **Governors:** Members of the school's governing body, including board members, trustees, and other individuals responsible for overseeing the school's operations and decision-making.
- **Staff:** Employees of The King's School Vattanacville, including teachers, administrators, support staff, and other personnel employed by the school.
- **Volunteers:** Individuals who provide services to the school on a voluntary basis, including but not limited to parents, alumni, and community members.
- **Contractors:** External individuals or organizations hired by the school to provide goods or services, including but not limited to IT providers, consultants, and service providers.
- **Parents:** Guardians or legal representatives of pupils enrolled at The King's School Vattanacville.

- **Pupils:** Students enrolled at The King's School Vattanacville, including both current and former students.

5. Roles and Responsibilities of Stakeholders

a) IT staff

Implement and Monitor Cyber Safety Measures: The IT Manager handles implementing and checking cyber safety measures to protect the school's digital infrastructure and data. To respond on time to any system leak or check the IT team must respond and provide the report to all staff using the ICT facilities.

Provide Training: The IT team must provide regular training and resources to educate the school community about cyber safety best practices. This includes providing quick alerts to the group in case of any social media hacking or cyber attack.

Manage Cyber Incidents: IT handles cyber incidents, including investigating and responding to incidents promptly.

Coordinate with Stakeholders: The IT must coordinate with other staff members, governors, volunteers, contractors, parents, and pupils to ensure compliance with the Cyber Safety Policy. Staff and Governors:

Compliance: All staff members and governors must follow the Cyber Safety Policy and take responsibility for their digital actions.

Reporting: Staff members and governors should report any suspicious activity or cyber incidents to the IT department at once.

b) Volunteers and Contractors:

Compliance: All volunteers and contractors must follow the Cyber Safety Policy and cooperate with the school's cyber safety measures.

Reporting: Volunteers and contractors should report any suspicious activity or cyber incidents to IT at once. It is essential for members of staff who suspect a cyber attack of any kind, to contact vith.doeurn@tksv.edu.kh ; please do not open emails or links that are suspicious or unrecognised. Report them to Vith Doeurn immediately.

c) Parents and Pupils:

Education: Parents and pupils should take part in cyber safety education programmes provided by the school and adhere to the guidelines outlined in the Cyber Safety Policy. Students who use any bypass (including purchased and unpurchased proxy servers) to try and crack the school network will trigger investigations by the IT team. Attempts, whether successful or not will be dealt with under the disciplinary policy.

Reporting: Parents and pupils should report any concerns or incidents related to cyber safety to IT at once.

d) All Members of the School Community:

Respect for Privacy: All members of the school community should respect the privacy and personal information of others and use digital resources responsibly. Data protection must not only guard against threats but also protect all members.

Cooperation: All members of the school community should cooperate with the IT Manager and other staff members to ensure the effective implementation of the Cyber Safety Policy.

Breaches of this policy will be subject to disciplinary, behaviour, staff discipline policies/ staff code of conduct.

6. Acceptable Use Policy

School Hardware and Software:

All hardware and software provided by The King's School Vattanacville must be used for educational and professional purposes only.

Users must not install unauthorized software or modify hardware configurations without permission from the IT department. Any system or module required for educational purposes must be properly requested and authorized.

Staff violations of the policy will be recorded and addressed by the disciplinary policy, behaviour policy, staff discipline policy, or staff code of conduct.

Materials:

The staff must not access, download, or distribute materials that are illegal, inappropriate, or infringe upon the rights of others. All materials created or shared using school digital resources must follow copyright laws and intellectual property rights.

Accounts:

Users must maintain the security of their accounts and passwords and must not share their login credentials with others.

Users must not try to gain unauthorized access to accounts, systems, or data.

Users are not allowed to log in to school accounts with anonymous devices or unauthorized internet providers or try to bypass a warning from the school AV protection alert.

It is recommended to update, at a minimum, your passwords every 6 months to ensure passwords are protected over the long term.

Social Media:

The use of social media on school premises or using school digital resources must follow the school's social media policy such as:

- Facebook Page
- School Web Portal
- School Website
- YouTube Channel
- School Instagram

Users should exercise caution when posting content on social media and must not engage in cyberbullying, harassment, or other inappropriate behaviour.

Other Systems:

Users must follow the acceptable use policies of any external systems or services accessed using school digital resources.

Users should report any security vulnerabilities or concerns related to external systems or services to the IT Manager at once.

Compliance:

All users of school digital resources must follow this Acceptable Use Policy and take responsibility for their digital actions.

Non-compliance with this policy may result in disciplinary action, including restriction of access to school digital resources, suspension, or termination of employment or enrolment depending on which step is breached in the HR code of conduct.

7. Cyber Safety Education

The King's School Vattanacville is committed to fostering a culture of cyber safety awareness among all members of the school community. The following initiatives and programmes will be implemented to educate and inform governors, staff, parents, and pupils about cyber safety:

Cyber Safety Training Programmes:

- **Staff Training:** Regular workshops and training sessions will be conducted for all staff members to educate them about current cyber threats, safe internet practices, data protection, and the school's cyber safety policies and procedures.
- **Pupil Education:** Age-appropriate cyber safety lessons will be integrated into the school curriculum to teach pupils about safe online behaviour, recognizing cyber threats, and protecting personal information. [This is encourage cooperation with ICT teachers and IT team.]

Awareness Campaigns:

- **Cyber Safety Week:** An annual Cyber Safety Week will be held to raise awareness about cyber safety issues through activities, presentations, and interactive sessions. All the KSV staff will be involved with this week.
- **Posters and Materials:** Informative posters, brochures, and digital resources will be distributed throughout the school to reinforce key messages about cyber safety. Given the large school staff and community, broadcasting cyber safety information is crucial to ensure everyone is informed and aligned.

Online Resources:

- **Cyber Safety Portal:** A dedicated section on the school's website will provide resources, guidelines, and tips on cyber safety for staff, parents, and pupils.
- **Regular Updates:** The IT department will provide regular updates on emerging cyber threats and best practices through emails, and the school's online platforms such as team groups or school telegram.

Safe Use of Social Media:

- **Guidelines:** As social media is such a popular medium of communication worldwide, we will make clear guidelines for the safe and responsible use of social media- this will be provided to all members of the school community.

Incident Response Training:

- **Simulated Exercises:** Regular simulated cyber incident exercises will be conducted to prepare staff and pupils for potential cyber threats and to practice the school's incident response procedures.
- **Response Teams:** Appointed cyber incident response teams will be trained to oversee and mitigate cyber incidents effectively.

Evaluation and Feedback:

- **Surveys and Feedback:** Regular surveys will be conducted to gather feedback on the effectiveness of cyber safety education programmes and identify areas for improvement.
- **Continuous Improvement:** The cyber safety education programme will be reviewed and updated regularly based on feedback and emerging trends in cyber safety.

In implementing these comprehensive cyber safety education initiatives, The King's School Vattanacville aims to empower its community with the knowledge and skills to navigate the digital world safely and responsibly.

Cyber Incident Response

The Cyber Incident Response Plan (CIRP) at The King's School Vattanacville is designed to effectively handle and mitigate cyber incidents, minimizing impact and swiftly restoring normal operations. It includes prompt detection, identification, containment, mitigation, eradication, and recovery of affected systems and data. Continuous monitoring and the use of security tools like school IDS and firewalls are crucial. Staff report suspected incidents to the IT department immediately, with incidents classified based on severity. An Incident Response Team coordinates the response, involving isolation of affected systems, malware removal, and patching vulnerabilities. Clear communication ensures staff, stakeholders, and the public are informed as needed.

There are two restore points in case the system is attacked. First, for online subscribed systems where all cybersecurity protection is under the provider, review contracts to understand the data loss or delay time to restore points. Ensure timely updates and provide a report to all impacted users. Second, for systems hosted locally (DC) with full administrative control, immediately restore from the last backup version and isolate the compromised version.

8. Data Protection

Data is the final document type, making its management and prevention crucial with an important level of security concern. Staff must adhere to the school policy and ensure it is practised and stored in a safe place. School data includes documentation, videos, audio, system credentials, licenses, software, links, and more.

- Ensure all personal and sensitive data is securely stored and accessed only by authorized personnel.
- Use encryption and other security measures to protect data, provided and designed by IT or through recommended methods.
- Regularly update software and systems to protect against vulnerabilities, as part of ISO/OS firmware security concerns.

For a clearer and deeper understanding, we will provide links to relevant points (9 ***Internet Usage and Data Security Protection ICT facilities.)*** in the IT Acceptance Policy.

Any breach of this policy will be addressed under the disciplinary policy, staff discipline policy/ staff code of conduct.

9. Monitoring and review

The school conducts regular monitoring and review of its Cyber Safety Policy to ensure its effectiveness and relevance in addressing emerging cyber threats. The IT Manager oversees this process and conducts annual reviews, considering feedback from the school community and changes in technology. Any updates or revisions to the policy are communicated to all stakeholders to ensure awareness and compliance. Feedback mechanisms are in place to gather input from staff, governors, volunteers, contractors, parents, and pupils, ensuring that the policy remains robust and responsive to evolving cyber risks. It should also be noted that the IT Team tracks and reviews all staff using the school system as a normal process to investigate system leaks or maintain system control.

10. Contact Information

On behalf of the IT department for any questions or concerns about the Cyber Safety Policy, please contact:

The revised version of the Cyber Safety Policy will be provided to all stakeholders after any updates or changes have been reviewed, approved, and implemented by the Principal. This process ensures that the policy remains current and aligned with the school's cybersecurity objectives.