SCHOOL OFFICE ORDER

BY

COLONEL BHUPENDER KUMAR, PRINCIPAL, SAINIK SCHOOL NALANDA

SSNL/4056/TRG/SOPs 08 May 25

STANDARD OPERATING PROCEDURE ON CYBER SAFETY & SECURITY

Appendix: - A

Introduction

1. Cyber safety is the safe and responsible use of Information and communication (ICT) technology. It is not just about keeping information safe and secure, but also about being responsible with that information, being respectful of other people online, and using good 'netiquette' (internet etiquette).

2. ICT devices have been provided in classrooms, labs and library for benefit of cadets. Internet access is also given to cadets as learning resource. However, these resources are to be used in a responsible and legal manner. Cadets must be aware about the rules on safe and right usage of digital infrastructure & facilities of School.

Aim

3. The aim of this SOP is to lay down guidelines for cadets about safe and secure use of internet and school's ICT devices installed in classrooms, labs and library.

Cyber Safety & Security

4. Rules to be followed by cadets while using ICT devices provided in classrooms, labs and library of school are listed below: as Do's and Don'ts:-

(a) DO's:

(i) Use ICT devices for academic or any authorized purposes only. It can be used only for research, information gathering and academic practice directly related to school assignments and extracurricular projects supervised by school faculty.

(ii) Handle equipment with care so that there is no damage to any hardware such as panels, keyboards, mouse, or monitors etc. and keep them clean.

(iii) Scan all external devices permitted by competent authority for malware before using them in any school systems.

(iv) Work collaboratively, but securely: If sharing work, ensure files are shared securely using school-approved platforms (e.g., cloud storage or internal systems).

(v) Report any un-serviceability to the IT department.

(b) DON'TS:

(i) Do not attempt to alter admin settings like changing configurations, installing unauthorized software or application, or tampering with hardware.

(ii) Do not bypass security measures: Do not attempt to disable antivirus, firewalls, or other security protocols.

(ii) Do not use school's ICT devices for non-academic activities or personal entertainment (e.g., gaming, social media, or unauthorized file downloads).

(iv) Do not use of the school network to access or process pornographic materials, sexually explicit material and files dangerous to any individual or group.

(v) Do not use external storage devices (USB drives, external hard drives, etc.) without prior approval, to avoid spreading malware or data breaches.

(vi) Do not access unauthorized content, browse or download from websites that may expose the school's network to malware or inappropriate content.

(vii) Do not transfer or store school data on personal devices.

(viii) Do not use personal or unsecured devices on the school network.

(ix) Do not engage in online discussions or activities that could harm the school's reputation.

5. Cadets must never indulge in cyber bullying. Sending, posting or sharing negative, harmful, false or mean information and content about someone is a serious offence which is punishable under Cyber law. Cyber bullying includes following:

(a) Posting nasty comments on somebody's posts or posts about someone.
(b) Creating someone's fake profile in his/her name and trying to defame someone.
(c) Sending threatening or abusive messages online or on the mobile phone.
(d) Excluding someone from online groups and forum.
(e) Putting embarrassing photographs without someone's permission.
(f) Spreading rumours or lies about someone on a site.
(g) Stealing someone's account password and sending unwanted/inappropriate messages from his/her account.
(h) Offensive chat.
(i) Creating fake online profile with intent to defame someone.

6. In case any cadet is facing cyber bullying, he/she must do following:

(a) Do not respond or retaliate by doing the same thing back.

(b) Take a screenshot of anything that you think could be cyber bullying and keep a record of it.

(c) If someone bothers you, make sure you block and report the offender to the social media platform.

(d) Never keep it to yourself. Report the matter to counseller, housemaster, teachers or school authorities.

7. Internet Safety guidelines to be followed by cadets are listed below as Do's and Don'ts:-

(a) **DO's**:

(i) Use the internet responsibly.

(ii) Log in securely: Use strong passwords and change them regularly.

(ii) Log out or lock devices when leaving them unattended to prevent unauthorized access.

(iii) Download only from trusted websites to minimize the risk of malware or viruses.

(iv) Beware of phishing websites check the URL to confirm if the website is secure (Look for HTTPS and a padlock symbol in the address bar before entering personal information).

(v) Be cautious about clicking on suspicious links in emails, websites, or pop-up ads or downloading attachments from unknown sources.

(vi) Be cautious with personal information: Only provide personal details (e.g., email, phone number) on secure, legitimate websites.

(viii) Report incidents: Any suspicious activity, cyber threats, or security issues should be reported immediately to the IT department.

(b) **DON'TS**:

(i) Do not share your credentials like usernames, passwords, or security codes with anyone.

(ii) Do not visit unsafe websites that could expose the school network to malware, phishing attempts, or other cyber threats.

(iii) Do not use public Wi-Fi networks for sensitive activities: Avoid accessing sensitive data or making online payments while connected to unsecured public Wi-Fi.

(iv) Do not share personal or financial information on insecure or suspicious websites.

(v) Do not download attachments from unknown emails: Attachments could contain malware or phishing attempts.

(vi) Do not use the network in a way that would disrupt the use of network by other users (eg. sending mass E-mail messages or annoying other users using unprofessional practices).

(vii) Do not share personal or confidential information via email or public file-sharing services like Google Drive, Dropbox, etc., unless authorized.

8. The IT department will regularly monitor the use of the school's digital resources and internet activity of cadets. It will determine whether specific uses of the network are consistent with the acceptable practices or not. It can recommend school authorities to restrict/terminate the privileges of a particular cadet who violates the norms and guidelines set up by the School.

9. The responsibility for use of Internet that does not comply with this SOP lies with the user to whom the account is registered and such cadets will be liable to compensate School for any direct loss or any consequential losses suffered by the breach of policy. School will review any alleged breach of this policy on case to case basis. Any violations of this SOP will also result in disciplinary action as per laid down rules.

10. Undertaking as per format given at Appendix A will be obtained from the Cadets and their parent/guardian at the time of admission. Cadets already studying in School and their parent/guardian will also be required to submit the said undertaking.

Conclusion:

11. By following the guidelines in this SOP, all users will contribute in maintaining a safe, secure, and efficient digital environment in School. It is essential for everyone to take responsibility for their actions and uphold the highest standards of cyber safety & security. This

SOP will be reviewed and updated as necessary to reflect changes in technology, school policies, and emerging cyber threats.

12. Extract of relevant paragraphs of this SOP will be hosted on school website for information of parents. All stakeholders are to adhere to various provisions laid out in this SOP. This SOP will supersede all instructions issued on this subject in the past and will be implemented with immediate effect.

(Bhupender Kumar)
Colonel
Principal

Distribution:

(a) Adm Officer
(b) Vice Principal
(c) Sr Master
(d) All House Masters
(e) All Class Teachers
(f) Main Office
(g) Office copy

Appendix- 'A'

(Refers to para 12 of SOP on cyber safety)

UNDERTAKING BY CADET

1. I have read and understood the provisions of cyber safety & security SOP and will abide by them. I further understand that any violation of any provisions of this SOP is unethical and may constitute a cyber offence. In case of any violation, my access privileges may be revoked and school can take appropriate disciplinary action.

2. I also declare that I shall not connect any school system to Internet through any unauthorized source. I further agree that I will not use Wi-Fi password, USB Drives/CD/DVD's or any other external storage device in any system of the school and I shall not open any attachments in any form that may spread virus and damage the network/ system.

Date: _____ (Signature of Cadet)

Cadet's Name: _____

Father's Name_____

Class: _____ Section: _____ Roll No: _____ House: _____

UNDERTAKING BY PARENT

1. As the parent/guardian of Cadet _____, I have read and agree to the provisions of cyber safety & security SOP. I understand that access to school's digital infrastructure is designed for educational purposes and Sainik School Nalanda has taken available precautions to monitor cadets' access.

2. I hereby give my permission to my ward to access school's digital infrastructure, after accepting cyber safety & security rules. I do understand that in case of any violation of this SOP by my ward, appropriate disciplinary action will be initiated by school authority which will be acceptable to me.

Date: _____ (Signature of Parent)

Parent/guardian Name: _____

Address: _____

Email id: _____

Contact Number: _____