RED ROSES PUBLIC SCHOOL

DIGITAL TECHNOLOGY

AND

SOCIAL MEDIA POLICY

2023

D - BLOCK, PALAM VIHAR, GURUGRAM, HARYANA – 122017

Under the aegis of Shri. R.R. Mehta Educational Trust

A Society registered under Societies Registration Act, 1860

Registration no S/12738 dated 13th July 1982

TABLE OF CONTENTS

PREAMBLE

As a private institution imparting public service, we are committed to conducting and governing ourselves with ethics, transparency, and accountability and to this, we have developed governance structures, practices and procedures that ensure that ethical conduct at all levels is promoted across our institution. In wake of the expansion of digital technology and reliance on digital resources and social media in COVID-19 and post COVID-19 era, the school has realized a need to develop its own digital technology and social media policy in view of the school's commitments stated above.

This policy seeks to lay down a code of conduct for the students and staff of the school while using digital resources available with them and while interacting on social media. While digital technology has transformed our society and has made interactions easier and swifter, it is the responsibility of the users of such resources and social media that they shall conduct themselves in a manner that upholds their own, as well as the school's reputation in the highest regard.

This policy focusses on issues such as cyber security, cyber bullying, cyber ethics, and etiquette and maintaining good practices. This School does not support or condone any behavior that is in violation of the law and specifically this policy. The management of the school is committed to providing its staff, employees, and students with a safe environment.

This policy provides for Suo motu regulation of the conduct of the users of digital technology and social media by the school and preparing adequate measures that may be taken for redressal of any violation of the policy.

APPLICABILITY

This policy will extend to all students, parents, staff members and employees of the school including those employed on contractual basis who are users of social media and digital technology.

SCOPE

The scope of this policy extends to all students, parents, staff members and employees of the school:

(a) Who use digital resources and social media platforms to interact with other students and staff members of the school.

(b) Who use digital resources and social media platforms to access any IT resources of the school.

(c) Who use digital resources and social media platforms to create, disseminate, transmit and store any content in respect of the school or its students or staff members;

(d) Who use digital resources and social media platforms to perform any task assigned to them as part of their curriculum or employment, as applicable.

DEFINITIONS

1. “Computer system” means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions.
2. “Cyber-crime” means any activity which takes place on or over the medium of computers, any electronic device like mobiles, tablets, laptops and smart devices, the internet or other technology recognised by the Information Technology Act. It includes any illegal activity where a computer or internet is either a tool, target, or both.
3. “Cyber/Online” abuse means any online behaviour that seeks to threaten, harass, harm, or humiliate a person using the internet, mobile technologies, or other digital services.
4. “Cyber security” means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification, or destruction.
5. “Data” means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network and may

be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

6. ‘Digital media’ means digitized content that can be transmitted over the internet or computer networks and includes content received, stored transmitted, edited or processed.
7. ‘Digital resource’ shall mean computer, computer system, computer network, data, computer data base or software
8. “Social media” means any platform which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify, or access information using its services.

CYBER BULLYING

Any act done by any user of a digital/computer resource and/or through any social media platform which is intended to humiliate, embarrass, threaten, intimidate any person or any other such purpose shall amount to cyber bullying**.**

Any act done by any user of a digital/computer resource and/or through any social media platform which may cause another person to do something that he/she may not do or cause another person to not do something that he/she may do in normal course, under a threat of any unpleasant, unlawful, or any form of injurious consequence shall also amount to cyber bullying.

The school students and staff members are mandatorily required to ensure that they do not indulge in any activity that amounts to cyber bullying. It shall be the duty of every user to report any incident of cyber bullying to the school so that appropriate action may be taken in accordance with this policy.

It may not be necessary to establish direct communication between the bully and the victim as even sharing of sensitive personal information about someone with a negative intent to a third person may amount to bullying.

Any person found indulging in an act done to support, abet or instigate cyber bullying shall be treated at par with the person who actually commits cyber bullying. The act of cyber bullying is also punishable by law under the Information Technology Act, 2000.

CYBER STALKING

Any act done by any user of a digital/computer resource and/or through any social media platform for the purposes of stalking, posting unwelcome comments, sharing pictures, repeating attempts to make contact which are not welcome, tracking updates of another user's usage of social media or digital resources and any other such similar act shall amount to cyber stalking.

The school students and staff members are mandatorily required to ensure that they do not indulge in any activity that amounts to cyber stalking. It shall be the duty of every user to report any incident of cyber stalking to the school so that appropriate action may be taken in accordance with this policy.

Any person found indulging in an act done to support, abet or instigate cyber stalking shall be treated at par with the person who actually commits cyber stalking. The act of cyber stalking is also punishable by law under the Information Technology Act, 2000.

When it is suspected that a personal electronic device such as a mobile phone or any other device is used to capture images of a crime (such as an assault), or contains any other evidence of a crime, the device will be confiscated and handed to the police.

If the Head of the School suspects an electronic crime has been committed, this will be reported to the Police Department. Where there is a further reasonable suspicion that evidence of a crime, such as an assault, is contained on a mobile phone or other electronic device such as a notebook, computer etc. and the device will be confiscated and handed to the investigating police officer. The police will determine any further action.

These actions may be taken even if the alleged incident occurs off site and/or out of school hours.

CODE OF CONDUCT

School students, staff members and employees of the school shall strictly abide by the following code of conduct failing which appropriate action may be taken in accordance with this policy:

(a) The students at the school should use digital technology and social media platforms primarily to enhance knowledge, to obtain positive influence, to help in academics, co-curricular and extra-curricular activities.

(b) No student/staff member shall create an anonymous profile on social media to contact any other student/staff member of the school in any manner whatsoever. Anonymous profiles, if any, shall immediately be deleted by such user.

(c) No student shall engage in any form of communication with any teacher or staff member over any social media platform such as Facebook, Instagram, Snapchat, Hike, Telegram, etc. such as sending friend requests, exchanging messages, making requests to follow etc.

(d) If any student is already in communication with any teacher or staff member over such social media platforms such as Facebook, Instagram, Snapchat, Hike, Telegram etc., they shall immediately withdraw and disable all such communications.

(e) No student, teacher, staff, or employee will click photographs inside the school premises and post them on their social media platforms without the consent of the head of the school or prior approval of the cyber committee.

(f) No student, teacher, staff, or employee will share pictures, videos, boomerangs, clips, GIFs, audios, or any other post related to school on any social media platforms.

(g) Any person found creating, managing, publicizing, talking about fake profile(s), fan page(s), funny or sarcastic meme page(s) or any humiliating, humorous, targeting, bullying, and/or defaming post or content related to school or its students', parents, staff and employees on any social media platform or via personal messages that are sent/created/forwarded etc. will also be considered as a part of cybercrime and will be reported. Above activity and/or promoting any such activity or case where person(s) was/were aware or hiding the cybercrime information will also be dealt with severe punishment under the IT Act and Cyber Crime Cell.

(h) Aiming to create a meaningful learning atmosphere in the school and particularly in the classroom, the school doesn't permit any student carrying any electronic article to the school. Non-compliance of the rules would be considered as an offence. If a student is found in possession of it, then the unauthorised electronic equipment would be confiscated and will be kept under school custody. Along with this, the school counsellor would also take parental undertaking from the parents, stating that the offence would not be repeated.

(i) The only acceptable form of communication between teachers and students or parents shall be through phone calls/email/SMS/WhatsApp Messenger and Microsoft Teams .

(j) No student, parent, teacher, staff, or employee will exchange monetary transactions in context of school purposes through cyber tools / practices that can lead to financial frauds and henceforth classified as a cybercrime.

(k) The contact details of the teachers or their social media profiles shall not be shared by any student at any cost with any third person unless it is with prior consent of the said staff member.

(l) The students, teachers and staff shall strictly ensure that there is no sharing, selling, or purchasing of any illicit, pornographic, or illegal content among them while using social media platforms and/or via email.

(m) The students, teachers and staff shall strictly ensure that they always remain courteous and polite in their conversations over social media platform with all individuals and every effort shall be made to ensure that there is no foul language used against any other user, especially when the interaction is between the students and/or staff of the school.

(n) No student or staff shall do any act that is against the terms of use and privacy policy of the social media platforms and that all the users shall ensure that they have fully read and understood the contents of the same before starting the use of such platforms.

(o) No student/staff member shall act/omit to act or aid or abet the commission/omission to abide by the provisions of the laws of India and especially the Information Technology Act, 2000 and the rules made thereunder.

(p) It shall also be the duty of every student/staff member to inform the Internal Complaints Committee or any staff member of the school in case any act in violation of this policy is found to be done to ensure that the school can provide a safe environment to the victim of the violation.

(q) Every student/staff member must pledge that they shall do every act to ensure that they remain compliant with the present policy and help create awareness regarding this policy among other students/staff members.

COMPLAINTS REDRESSAL MECHANISM

All or any complaints made by any student or staff regarding the violation of any of the provision of this policy or regarding any harassment of any kind over any social media platform which is done or aided or abetted by any other staff member/student at the school shall be adjudicated upon by the Internal Committee set up by the School under the Anti Sexual Harassment Policy, 2017.

The provisions for grievance redressal mentioned in the Anti Sexual Harassment Policy, 2017 regarding process of filing complaint and process of enquiry will apply Pari Materia to the present policy in so far as practical and possible.

The Internal Committee shall be empowered to address issues regarding cyber bullying, cyber stalking, and violation of the code of conduct under this policy. Considering the gravity of the violation by the student/staff member, the Committee shall be empowered to take any decision, including but not limited to:

(a) Expulsion from School

(b) Suspension for a period deemed fit ranging from 1 day to up to 10 weeks.

(c) Demotion of the staff member/withdrawal of pecuniary benefits.

(d) Compensation to the victim of the violation

CYBER SAFETY COMMIITTEE

Any case of cyber safety, cyber bullying, cyber stalking, cyber fraud and or any other concern, crime or incident related to cyber safety that needs to be reported or discussed can be brought to the knowledge of the following persons:

1. Head of the School : Mrs. Ritu Bedi
2. Headmaster : Mr. Pankaj Mahajan
3. Cyber Cell In-charge : Ms. Praveen Yadav
4. Administrative In-charge : Ms. Kruti Salwan
5. Counsellor & Psychologist : Ms. Christymol Philip
6. Sports In charge : Mr. Shankar Mahto

The above committee shall be functionally responsible and take all actions necessary for cyber security and safety in the interest of the affected student, teacher, employee, staff, parent, and the school.

The students, parents, employees, and staff are encouraged to share cybercrime related personal information with any other school member also who they feel confidant & comfortable with and who can further report the issue to the committee for appropriate action.

MISCELLANEOUS

Every student/staff member who is a user of digital technology and social media platforms in any capacity shall also ensure total and strict compliance with the provisions of the Information Technology Act, 2000 and the rules made thereunder, failing which they shall be liable to be proceeded with under the provisions of this policy if a complaint is received in that regard.

The school reserves the right to amend, abrogate, modify, rescind /reinstate the entire policy or any part of it at any time.

All parents are welcome to visit the school to discuss any issues that they may have regarding their ward, or school facilities, in context of cyber security and safety after taking prior appointment from the concerned staff/teacher/principal of the school.

FOR SAFE USE OF INTERNET ALWAYS FOLLOW THESE POINTS:

- Must receive permission from a member of staff before accessing the internet.
- Must access only appropriate sites for their work; any attempt to bypass filtering system or access social networking sites or chat rooms will be with the permission of a teacher for a work-related item.
- Must not claim to be representing the school in an official capacity when using the internet or e-mail or website privately.
- Must not use any internet services to purchase goods or make any payments unless authorised otherwise.
- As the internet allows you to do more and more online, it is extremely important to be aware of the dangers and how to stay safe.
- Use social networks' privacy settings so only your friends can see your information.
- Never open an email from an unknown source – it may contain viruses that can harm a computer. And don't access or use files without the permission of owner.
- Don't send pictures to strangers or view pictures that strangers send you.
- Passwords should be kept private (except from parents).
- Always use the two-factor authentication for email and other important logins.
- Never give out personal details like in messenger or in personal profiles.
- Never give a friend's details and never share your password with anyone and even enter it carefully, if someone is sitting near you.
- Never meet up with anyone you befriend online.
- Never open the emails \ attachments \ links coming from any unknown person.
- Be careful while sharing your photos on social media or with anyone.
- Never try to login as someone else and read their emails or access other's data.

Cyber Safety and Security

Guidelines for School

विद्यया ऽ मृतमश्नुते

एन सी ई आर टी
NCERT

Be safe in the cyber world ...

Cybersafety is the safe and responsible use of information and communication 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 practising good 'netiquette' (internet etiquette).

As information infrastructure and Internet became bigger and more complex , it became critical to maintain systems functional and alert to security issues. Though the system administration tasks have become easier in recent years, school administrators need to be more updated on the systems and network security In recent years, all systems are exposed to Internet; hence there is increased challenge in maintaining and protecting them from the attackers.

Schools play a key role in promoting internet safety. Schools are primarily responsible for keeping systems/ computers/ network devices secure and functional. It is important to keep the information as secure as we keep the systems and network devices in the organisation.

Index

1. Identify threat vulnerability & assess risk exposure
2. Develop protection & detection measures
3. Protect sensitive data
4. Respond to and recover from cyber security incidents
5. Educate your stakeholders

Identify threat vulnerability & assess risk exposure

1

- Slow and sluggish behavior of the system.
- Inexplicable disappearance of system screen while working.
- Unexpected pop ups or unusual error messages.
- Drainage of system battery life before expected period.
- Appearance of the infamous BSOD (Blue Screen of Death).
- Crashing of programs/ system.
- Inability to download updates.
- Navigation to new browser homepage, new toolbars and/or unwanted websites without any input.
- Circulation of strange messages from your email id to your friends.
- Appearance of new , unfamiliar icons on Desktop.
- Appearance of unusual message or programs which start automatically.
- Unfamiliar programs running in Task Manager.

2 Develop protection & detection measures

- Invest in a robust firewall.
- Have students and teachers create strong passwords.
- Have a password protocol that specifies strong password guidelines, frequent change of passwords, avoid reuse of old passwords.
- Use only verified open source or licensed software and operating systems.
- Ensure that computer systems and labs are accessed only by authorized personnel.
- Discourage use of personal devices on the network, such as personal USBs or hard drives.
- Set up your computer for automatic software and operating system updates.
- Check that antivirus software in each system is regularly updated.
- Consider blocking of file extensions such as .bat, .cmd, .exe, .pif by using content filtering software.

Develop protection & detection measures

2

- Read the freeware and shareware license agreement to check if adware and spyware are mentioned, before installing them on systems.
- Use encryption such as SSL or VPN for remote access to office or school lab, through internet.
- Ensure that third-party vendors (who have contract with the school) have strong security measures in place.
- Consider contracting with a trusted / verified third-party vendor to monitor the security of your school's network.
- Institute two or multi factor authentication for students, teachers and administrators when they log on.
- Protect your Wi-Fi Connection with secure password, WEP encryption, etc.
- Encrypt the network traffic.
- Change the administrator's password from the default password. If the wireless network does not have a default password, create one and use it to protect the network.
- Disable file sharing on computers .
- Turn off the network during extended periods of non-use etc.
- Use "restricted mode", "safesearch", "supervised users" and other similar filters and monitoring systems, so that no child can access harmful content via the school's IT systems, and any concerns can be detected quickly.

3

Protect sensitive data

- Design and implement information security and access control programmes and policies by evaluating the storage (used/ unused), access, security and safety of sensitive information.
- Never store critical information in system's C drive.
- Backup critical data (contact numbers, email IDs, aadhaar number etc.) in an off-site location.
- Establish safe reporting guidelines and escalation methods to protect the identity of the person who reports the breach of security.

4 Respond to and recover from cyber security incidents

- **Initial assessment**: To ensure an appropriate response, it is essential that the response team find out:
  - How the incident occurred ?
  - Which IT and/or OT systems were affected and how ?
  - The extent to which the commercial and/or operational data was affected ?
  - To what extent any threat to IT and OT remains ?

- **Recover systems and data**: Following the initial assessment of the cyber incident, IT and OT systems and data should be cleaned, recovered and restored, as much as possible, to an operational condition by removing threats from the system and restoring the software.

- **Investigate the incident**: To understand the causes and consequences of a cyber incident, an investigation should be undertaken by the company, with support from an external expert, if appropriate. The information from an investigation will play a significant role in preventing a potential recurrence.

- **Prevent re-occurrence**: Complying with the outcome of the investigation mentioned above, any inadequacies in technical and/or procedural protection measures should be addressed, in accordance with the company procedures for implementation of corrective action.

5

Educate your stakeholders.

- Frame cyber safety rules as Do's and Don'ts for the Schools.
- Orient school administrators with latest tools that can be used to monitor the sites visited by the students/ teachers.
- Orient the stakeholders on cyber laws (http://cyberlawsindia.net/)
- Consult cyber security professionals to raise awareness levels about the risks in cyber space and their preventive measures
- Introduce courses/ lessons/ activities for students and teachers on major components of cyber security and safety.
- Advocate, model and teach safe, legal, and ethical use of digital information and technology.
- Promote and model responsible social interactions related to the use of technology and information
- Celebrate Safer Internet Day (February 5th) and conduct activities to create awareness through cyber clubs
- Establish a relationship with a reputable cybersecurity firm/ organisation.
- Follow guidelines, policies and procedures to keep the school safe and secure in cyberspace.


CYBER SECURITY
PROTECTING
SAFE PRACTICE
MAJOR THREATS
Cyber Crime
Information & Devices
Unauthorised Access
Modification
Destruction
Disruption
Disclosure
Use/Misuse
Theft
Curiosity
Money
Revenge
Attention
Fun
Fake Account
Identity Theft
Pornography
Slander
Libel
Defamation
Cyber Stalking
False Accusations
including
Repeated Harassment
Websites
IM
through
E-mails
Phone
Online Groups
Insults
Teasing
Name Calling
Lies
Rumors
Threats
Threats
Cyber Bullying
Sexual Activities
Grooming
Harassments
Online Predators
committed for
from
include
Share
Changed
should be
do not
Securely
save
Password
Strong
shoud be
Firewall
Password
protect
use
Software
update
Data
backup
Desktop/ Laptop
Pirated Software
no to
use current/ updated
use & update
Antivirus
Operating System
regular/ automatic
Scan
Cyber Laws
use
for
legal
in
Latest Browser
Content Filtering
WiFi
secure
E-mail Tracer
Internet
update
Browser Pluggins
Friendship
avoid
with
Unknown People Online
in using
Copyright Violation
Before Discarding
format
Authorised Store
Mobile Devices
download app from
Sensitive Information
obtaining
through
Social Engineering
uses
Scareware
Virus
Spyware
include
Ransomware
Worms
Trojans
Adware
Phishing
Scam
Hacking
Malware
Spam
Piracy
Website Defacement
E-Mail Bombing
Morphing
Hoax
means
Social Media
any
Threats
check
URL
inform
Parents
beware of
Spy Camera
do not open
clean
E-mail Attachments
avoid
Referral Links
from
Unknown Persons
Untrusted Website
never visit
Meeting in Person
avoid
Call from Weired Number
do not accept
Call back
and do not
switch on
Type the URL
instead
Bluetooth
only
When Needed
record
IMEI Number
Authorised WiFi
Auto Lock
use
access only
like
Phone Call
Tab Napping
Instant Messaging
Password
User Name
Credit Card Details
Click jacking
E-mail Spoofing
Websites Spoofing
Strangers
avoid
do not share
Personal Informtion
use
Privacy Options
Security Options
ensure
User to be Old Enough
approach
Cyber Police
save
Chat Screen
Be Scared
browser's cookies and cache
CC:BY:SA-M.U.Paily