XLS Virtual Learning: Cyber Safety Guidelines

The purpose of this document is to provide advisory to parents, staff and students for Virtual Learning so that they remain cyber safe. The document also provides guidelines for non-negotiable behaviours by all stakeholders so that effective teaching and learning can take place. In particular, this document aims to promote the following goals:

- to ensure that Virtual Learning platforms are used for their intended purposes and all the stakeholders comply to the non-negotiable practices
- to provide guidance on the usage of these platforms so that all the stakeholders are cyber safe
- to make them aware of key IT laws and the related implications

Please note that the School's IT and Acceptable usage policy and Behavior Management policy applies to all the Virtual Classrooms. Any suspected violations may be reported to a teacher, counselor or School administrator in person/ email and the confidentiality of the report will be respected. The School ensures a proper handling of the issue and will engage with the School counselor, parents, staff and students depending upon the incident.

Non-negotiable Practices

- Parents/Students/Guardians must not share class invites/ links with anyone who is not a part of the school or class or has not been invited by the teacher.
- Parents/Students/Guardians must not take photos, screenshots, record videos/ audios of the virtual sessions.
- All material shared on Managebac, Teamie and Google Hangouts is the School's intellectual property and downloading/ circulating/ sharing of content without permission is strictly prohibited.
- Staff, parents and students must keep their identity safe and not share google passwords or their identity with anyone. Staff, parents and students must ensure they sign out of each session completely after completion of the session.
- Social media apps such as SnapChat, Instagram, WhatsApp, or Facebook are not official, School-sanctioned channels of communication and must not be used for teaching and learning.
- Parents/Students/Guardians should inform the Teacher/School formally, in case a student is not able to attend any session.

- All users are required to be polite, respectful, and appropriate in their communications and must represent the school's values in their interactions with others, this applies for written words and as well as tone of conversation.
- The users(staff/students) must respect copyright and licensing laws with respect to software, information and other materials retrieved from the Internet.
- Users must not indulge in cyber bullying and writing of unkind remarks on the walls of unsuspecting friends, sharing of pornographic material through social media and/or email.
- The hacking and attempts at hacking the School personnel's email accounts, network and any other school assets have been and will continue to be dealt with the necessary seriousness.

Students have to comply with the School's behaviour management and Acceptable Usage policy while they are online.

Cyber Safety Advisory

Since students will be spending time online, parents are requested to speak to them regarding the importance of staying safe in the cyberworld. Parents should be aware of Online Frauds happening in Virtual World. Some of the examples are given below:

- Fraudsters try following tricks to cash in on the Coronavirus fear.
- Malware attacks disguised as sensationalized COVID-19 news or Charity pleas
- Coronavirus-themed spam spreading malicious malware.
- COVID-19 themed phishing emails impersonating Centers for Disease Control & Prevention.
- A global email phishing scam carrying the logo of the WHO.
- Malicious coronavirus map hiding info-stealing malware etc.

Parents should keep the viral attacks at bay and disinfect their child(ren)'s system. They should take the following steps to stay protected:

- Safeguard your children's devices from such COVID-19 malwares, install reliable and updated antivirus and anti-spyware.
- Ensure that the websites they use are authentic and encrypted with https in URL.
- A safe practice would be to type the URL on the browser instead of clicking on links sent to you through email, chat or any other way.
- Do not use public Wi-Fi or any open network.
- Do not download any app from an unknown source, link.

- Do not authorize any transaction without verifying properly.
- Do not share your personal and financial details along with OTP
- Do not download any app from an unknown source, link.
- Create a strong password using a combination of numbers, punctuation marks, letters etc. and change your password regularly

Please guide your child through the following guidelines:

Be a Cyber Smart Citizen

- Be vigilant: Visit safe sites which are age appropriate and approved by your parents and teachers. Do not open emails from unknown email ids. It is strongly advised that no face-face meeting is arranged with a person that a student knows only through emails/ internet.
- Be cautious: Make good choices when you are online. Share only information that is required and safe to share. Make sure that you log out after your work is done. Do not share your password with anybody.
- Be respectful: Be kind and respectful to others when you are online. Promise to THINK – True, Helpful, Inspiring, Necessary, Kind.
- Be vocal: Tell your parents and teachers if someone is being hurtful or unkind online or sharing disturbing content. Stand up to Cyber Bullying and remember that your digital presence should not hurt others.
- Be safe: Use safe Wifi networks and keep your device safe and secure at all time.
- Be honest: Always follow copyright laws and remember to cite the sources that you use for your work.

Current circumstances may have an impact on social and emotional health of students. Some of them may feel isolated or anxious. Please ensure that they should contact teachers and/or counsellors if there is such a need.

Appendix A – Some Law-Breaking Examples

- Creation of a False Electronic Record to cause damage or injury: Section 463 of the Indian Penal Code, 1860
- Punishment of Forgery, i.e. creation of False Electronic Record: Section 465 of the Indian Penal Code, 1860
- Forgery for purpose of harming reputation: Section 469 of the Indian Penal Code, 1860

- Using as genuine a forged document or electronic record: Section 471 of the Indian Penal Code, 1860
- Punishment for sending offensive messages through communication service, etc.– Section 66A of the Information and Technology Act, 2000
- Faking Name/ Identity – Section 66 D of the Information and Technology Act, 2000Hacking someone's Account and using it – Section 66 C of the Information and Technology Act, 2000
- Person making a Fake Account with Someone else name or PIC- Section 66D of the Information and Technology Act, 2000
- Posting/Sharing/Forwarding Obscene Content – Sec 67 of the Information and Technology Act, 2000
- Posting/Sharing/Forwarding Vulgar Inappropriate Content- Sec 67A of the Information and Technology Act, 2000
- Posting/Sharing/Forwarding Non-Consensual Private Images/Videos- Sec 66 E and Sec 67 A or Sec 67B of the Information and Technology Act, 2000

Appendix B - Key IT Act Laws

- Section 463 of the Indian Penal Code, 1860 deals with whoever makes any false document or false electronic record or part of a document or electronic record, with intent to cause damage or injury], to the public or to any person or with intent to commit fraud or that fraud may be committed, commits forgery.
- Section 465 of the Indian Penal Code, 1860 deals with whoever commits forgery shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.
- Section 469 of the Indian Penal Code, 1860 deals with whoever commits forgery, [intending that the document or electronic record forged] shall harm the reputation of any party, or knowing that it is likely to be used for that purpose, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine.
- Section 471 of the Indian Penal Code, 1860 deals with whoever fraudulently or dishonestly uses as genuine any [document or electronic record] which he knows or has reason to believe to be a forged [document or electronic record], shall be punished in the same manner as if he had forged such [document or electronic record].
- Section 66A of the IT Act deals with any person who sends, by means of a computer resource or a communication device,–

- (a) any information that is grossly offensive or has menacing character; or
- (b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device;
- (c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine
- Section 66C of the Information and Technology Act, 2000 Act deals punishment for identity theft and says that whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh.
- Sec 66D of the Information and Technology Act, 2000deals with punishment for cheating by personation by using computer resource, with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.
- Section 66E of the Information and Technology Act, 2000- whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.
- Section 67 the Information and Technology Act, 2000: Punishment for publishing or transmitting obscene material in electronic form. Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.
- Section 67A of the Information and Technology Act, 2000- Punishment for publishing or transmitting material containing sexually explicit act, etc., in electronic form. -Whoever

publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees

- Section 67B of the Information and Technology Act, 2000 deals with whoever,–
  (a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or
  (b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or
  (c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or
  (d) facilitates abusing children online, or
  (e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Disclaimer:- As all systems and control of the said systems remains solely with the parent(s)/ teacher(s)/staff and/or student(s) on which E-learning facilities are being accessed and/or disseminated and not within the control of the School and/or its server, the School shall not be responsible for any claims/losses/ consequences/etc. of any incident of hacking, improper and/or unauthorised access, phishing and/or any such incident and each parent(s) is strongly recommended to take independent steps, in addition to following the above recommended advisory, to ensure safe and secure usage of the electronic devices to avail E-learning Facilities.

Acknowledgement

We would like to thank Mr. Rakshit Tandon, Cyber Safety Expert , Consultant- Internet and Mobile Association of India, Director/Co-Founder – HACKERSHALA/CODESNAG for his guidance.