Mallya Aditi International School

e-Protection Policy

Mallya Aditi International School is committed to providing an atmosphere that is inclusive, non- threatening and safe, one that promotes student learning and personal growth. The school will take all reasonable measures to protect every student from online harm, and will deal appropriately and sensitively with complaints of unsafe behaviour online. This policy, in conjunction with the school's Child Protection Policy and Anti-Bullying Policy will address online safeguarding and protection issues.

This e-Protection Policy contains the following sections:

1. Purpose
2. Nature of Online Risks
3. Key Responsibilities of Different Stakeholders
4. Reporting Procedures
5. Preventive Measures
6. Appendix

1. Purpose of the Policy

The purpose of this policy is to establish effective, responsive and inclusive processes to ensure the online safety of the school community. The policy also recognizes the power of digital media and technology as tools for learning and seeks to create a culture and infrastructure that requires members of the school community to be discerning, ethical and responsible digital citizens. The policy seeks to empower the school community in its safe use of digital technology by laying out clear responsibilities for stakeholders and establishing procedures for reporting and responding. It emphasises the need for rigorous preventive measures at structural and systemic levels that would mitigate online risks and build an informed community of learners.

2. Nature of Online Risks

Online risks include risks of
3.1. Content
3.2. Contact
3.3. Conduct
3.4. Contract

Within each area of risk lies the possibility of the risk carrying aggressive, sexual or value-laden connotations. The list below is not exhaustive. An appendix (A.1) carries definitions of some of the lesser-known terms mentioned in this section of Online Risks.

3.1. Content- wherein a child engages with/ is exposed to potentially harmful content online e.g. violent, gory, graphic, racist or extremist information and communication, pornography, sexualization of culture, oppressive body image norms, mis/disinformation, age-inappropriate marketing of user-generated content.

3.2. Contact- wherein a child experiences or is targeted by potentially harmful adult contact e.g. harassment, stalking, unwanted or excessive surveillance, sexual harassment, sexual grooming, sextortion, the generation and sharing of child sexual abuse material, ideological persuasion or manipulation, radicalisation and extremist recruitment.

3.3. Conduct- wherein a child witnesses, participates in or is a victim of potentially harmful peer conduct e.g. bullying, hateful or hostile communication or peer activity, sexual harassment, non-consensual sexual messaging, adverse sexual pressures, potentially harmful user communities (self-harm, adverse peer pressure)

3.4. Contract- wherein a child is party to or exploited by potentially harmful contract e.g. identity theft, fraud, phishing, scams, hacking, blackmail, security risks, trafficking for purposes of sexual exploitation, streaming child sexual abuse, gambling, filter bubbles, micro-targeting, dark patterns shaping persuasion or purchase.

(Reference source for this section-CO:RE Project https://doi.org/10.21241/ssoar.71817)

3. Key Responsibilities of Different Stakeholders

This section includes responsibilities of:

4.1. Child Protection Committee
4.2 Child Protection Officer
4.2. Non- Teaching Staff
4.3. Teachers
4.4. System and Network Administrators
4.5. Parents
4.6. Students

4.1. Child Protection Committee is to:

- Promote an awareness and commitment to online safeguarding throughout the school community
- Ensure that online safety education is built in/ embedded across the curriculum
- Facilitate training for the staff and others working in the school
- Be aware of emerging online safety issues and engage in identifying preventive measures

4.2 Child Protection Officer is to:

- Maintain accurate, confidential and secure records for all incidents that involve the use of technology to cause harm to another student/s, staff member/s or the institution.
- Provide support and advice to staff when an issue of online child protection arises.
- Follow process as listed in the school's Child Protection Policy to address online incidents of harm.
- Alert the school's System and Network Administrators if harm across the school's network has been reported.

4.3. Non- Teaching Staff are to:

- Read, understand, adhere and promote the school's e-Protection Policy and Child Protection Policy.
- Be aware of online safety issues related to mobile phones, laptops and other devices, and that they would be monitored by the school according to the e-Protection Policy.
- Refer to the reporting procedures to report any suspected misuse or problem.
- Maintain awareness of current online safety issues and initiate dialogue and discussion regarding the same.
- Model safe, responsible and professional behaviours in their own use of technology.
- Ensure that any digital communication with students is professional in nature and only through school based systems.

4.4. Teaching Staff are to:

- Ensure that online protection procedures are embedded in all aspects of the curriculum and other school activities.
- Install and update safety applications on the devices that they use for school.
- Screen applications, platforms, websites and links for safety threats before sharing them with students.
- Monitor, supervise, guide and support students engaging in digital activity in lessons, extracurricular and extended school activities.
- Ensure that during lessons where internet use is pre-planned students are guided to sites checked as suitable for their use and that processes are known and used when dealing with any unsuitable material that is found in internet searches.
- Store student work in secure locations.
- Report security breaches, or incidents related to cyber-bullying to their Section Head/ Coordinator.

These are in addition to the responsibilities laid out in the above section on responsibilities for Non-Teaching staff.

4.5. System and Network Administrators are to:

- Read, understand and act according to the reporting procedures in case of abuse, misuse or access to inappropriate materials.
- Register devices onto the school network in order for users to gain Wi-Fi access
- Maintain IT systems (servers, networks etc.) and hardware within the school campus
- Ensure the installation of Firewall hardware to protect devices using the school network
- Install and monitor DNSFilters (software) on portable devices used by students - this ensures that restrictions remains in place regardless of the network being used by the device
- Install and monitor Anti-Virus software on school managed devices
- Create secure email accounts for teachers across the school and for students from grades 6 to 12
- Troubleshoot and respond to concerns as and when they arise
- Report to Section Head/s, any breaches of safety, or harm that was observed across the school network, or on any of the school devices.

4.6. Parents are to:

- Familiarize themselves with, and endorse the school's e-Protection Policy and iPad/ Internet Policy. Parents are urged to recognize that the safety of children online is a collaborative effort and requires parental involvement.
- Support the school in promoting online safety, which includes students' use of the internet, devices, photographs and videos.
- Recognize the role of parent supervision, digital contracts, dialogue and consequences in helping children stay safe online.
- Understand the importance of, and assert age-restrictions on games, shows, and social media platforms.
- Consult the school if they have any concerns about their children's use of technology
- Report online incidents as soon as possible, as per the procedure listed in the e-Protection Policy.
- Participate in school-led activities that relate to the online safety of children.
- Model appropriate and safe online behaviour for their children e.g. not sharing their passwords with children, ensuring emails of parents are kept private etc.
- Engage with the children on the apps that they use and the content they access. For younger children, supervision is recommended. As children move into adolescence, supervision might not be practical, and open conversations about how children access technology is important and necessary. Building in online dangers, and digital etiquette into these conversations is strongly recommended.
- Ensure that they themselves do not use the internet/ social network sites/ other forms of technical communication in an inappropriate or defamatory way

4.7. Students are to:

- Use internet and technological devices in accordance with the iPad/ Internet Policy (which they and/ or their parents are required to sign) and the e-Protection Policy.
- Know and understand online risks (content, contact, conduct and contract) and the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology (refer to Reporting Procedures)
- Know and understand school procedures on use of digital devices, taking/use of images and videos, and cyber bullying
- Understand the importance of adopting appropriate online safety practice while using digital technologies outside of school and realise that the school's e-Protection Policy covers their actions outside of the school, if related to their membership of the school.
- Help the school in the creation/ review of the e-Protection Policy and its procedures.

5. Reporting Procedures

This section has information on
5.1 What Constitutes an Online Incident
5.2. Reporting Process
5.3. Consequences for Unsafe Online Behaviour by Students

5.1. What Constitutes an Online Incident

An Online Incident is said to have taken place if any member of the school community reports any of the behaviours listed in section 3 of the policy. This policy does not extend to students engaging in academic malpractice using electronic means. Incidents of academic malpractice should be reported to respective Heads of Sections and the Principal.

It is important that all incidents be reported to school.

5.2. Reporting Process

Students, parents and staff are required to report incidents of online harm at the earliest possible.

For students

- Students can report an incident to a Teacher, Counsellor, Section Head, Principal or any other staff in school whom they feel safe with.

For parents

- Parents can report incidents to the student’s Class Teacher, a Counsellor, relevant Section Head, or Principal.

School is in the position to act on complaints that involve unsafe behaviour by members of the school community. Should the unsafe behaviour be perpetuated by individuals outside of the school community, parents are encouraged to register their complaints with the Cyber-police.

5.3. Consequences for Unsafe Online Behaviour (By students)

Consequences for engaging in unsafe behaviour online will be decided by school administration.

For complaints of a sexual nature, the POCSO Act, 2012 could apply in which case, the handling of the complaint no longer remains within the control of the school. Consequences will, in these cases, be determined by the concerned legal authorities. If parents report other incidents of a non-sexual nature to the Cyber-police, the handling of such complaints will move out of the jurisdiction of school.

6. Preventive Measures

The school takes safety and security of its network and devices seriously. Several measures, as listed below are in place and are actively implemented. We do recognize however, that security threats arise despite all reasonable efforts. In order to continue to safeguard our students the school requires parents and students to share concerns and incidents as and when they arise.

- School has appointed two dedicated System and Network Administrators (their role has been detailed in section 4.5. Device specific technical support is also available to teachers and parents for school managed devices through contractual arrangements.
- School-authorized student email accounts have been created for students, solely for educational purposes, from grades 6 to 12. These accounts have restricted access. Students cannot mail, or receive emails from individuals outside school.
- Visitors/guests who need to use the school’s networks, will abide by this policy.They cannot access the school network without being authorized to do so by the System and Network Administrators.
- School managed devices have safety checks and age-appropriate restrictions installed. AI-powered DNS filters are installed, which protects users from accessing malicious, harmful and suspicious sites.
- Students are required to sign off on an iPad/ Internet Policy which clearly lists behavioural expectations from students while using technology for learning. This policy is also shared with the parent.

- Staff members are bound by a Code of Conduct that prevents them from communicating with students on social networking sites and from using technology to access, produce or distribute any information or violent or sexual images that are harmful for children.
- Digital images/ videos of students are not to be shared on social media by teachers.
- Students are not allowed access to their mobile phones while in school, unless permitted to do so, by teachers, for educational purposes.
- Digital Citizenship and Safety has been incorporated into the school-wide Personal and Social Education (PSE) programme.
- Teachers review online content, applications before sharing them with students.
- Reported incidents are dealt with immediately, and sensitively.
- Regular awareness and skill building sessions on online safety are conducted with the parent community so that they remain vigilant and equipped to handle challenges and concerns outside of school.
- Incident records and other sensitive information are maintained according to school mandated standards of confidentiality and security.

This policy will be updated every two years.

Resources

Parents and staff are encouraged to visit the following websites to enrich their understanding of online safety:

- https://www.commonsensemedia.org/
- https://www.itu-cop-guidelines.com/parentsandeducators (Guidelines for Parents and Educators on Child Online Protection 2020, International Telecommunications Union, United Nations)
- https://ncpcr.gov.in/ (Being Safe Online, National Commission for Protection of Child Rights, Government of India)
- https://www.gov.uk/government/publications/keeping-children-safe-in-education--2 (Keeping Children Safe in Education 2021, Department of Education, UK)
- https://www.saferinternet.org.uk/advice-
- http://www.childnet.com/parents-and-carers/hot-topics

Appendix

A.1. lists definitions of some of the lesser known Online Risks (Section 3)

Body image norms are societal standards (values and beliefs) about physical attractiveness. These understandings tend to be implicit and pervasive.

Dark pattern is a user interface that is carefully crafted to trick or mislead users into doing something that they might not otherwise do. E.g., buying insurance with their purchase, signing up for recurring bills.

Disinformation is a type of misinformation that is intentionally false and intended to deceive or mislead.

Filter bubble is the intellectual isolation that can occur when websites make use of algorithms to selectively assume information a user would want to see, and then give the information to the user according to the assumption. Websites make these assumptions based on information related to the user, including former click behaviour, browsing history, search history and location. E.g., personalised search results on Google

Ideological persuasion or manipulation is the usage of information, incentives and even coercion to change user behaviour. Behaviour-oriented designs persuade users to buy more (one-click checkout) or stay logged in (manipulating social media news feeds).

Microtargeting or micro-niche targeting is a marketing strategy that uses consumer data and demographics to identify the interests of specific individuals or very small groups of like-minded individuals and influence their thoughts or actions. E.g., political campaign managers collecting detailed information about individual voters to send specific messages and influence voter's decision making.

Misinformation refers to false or out-of-context information that is presented as a fact, regardless of an intent to deceive.

Online radicalisation is the process whereby individuals through their online interactions and exposures to various types of internet content, come to view violence as a legitimate method of solving social and political conflicts.

Phishing is the fraudulent practice of tricking internet users (through deceptive email, messages or websites) into revealing personal or confidential information which can then be used illicitly

Sextortion is the practice of extorting money or sexual favours from someone by threatening to reveal evidence of their sexual activity.

Sexualization of culture refers to the dramatic increase in the appearance of sexualised images in advertising, mainstream media, and other venues of popular culture.

User-generated content (UGC) is original, brand-specific content created by customers and published on social media or other channels, and is used across all stages of the buyer’s journey to influence engagement and increase sales. E.g., unboxing videos, reviews, testimonials, etc.