EMINENCE PRIVATE SCHOOL
مدرسة أيمينينس الخاصة

Online Safety Policy

Version 4.0

POLICY	ONLINE SAFETY POLICY
STATUS	Implemented
FOCUS	School's online safety norms
RESPONSIBILITY	School leadership and Online Safety Group
APPLICABILITY	School community
DATE OF REVIEW	FIRST REVIEW: September 2020 SECOND REVIEW: Feb 2021 THIRD REVIEW: March 2022 FOURTH REVIEW: June 2023 NEXT REVIEW: June 2024

Policy Objective

The Online Safety Policy provides an insight into the overall safety norms when technology is used in the different domains of the school. This policy is designed to demonstrate and implement good and safe digital practices for all staff, students and parents.

Rationale

Technology has arrived to stay. Its impact on education has been profound and this has increased many folds ever since the pandemic of 2020. Overnight all of education moved into online mode without much prior knowledge and unaware of the perils. And there is no denying that the changes that education has seen over the last year is here to stay. However, over the months that have passed, the understanding of online technology has improved and the realization that this requires a strong footing in safety and security has also become evident. In such a situation it becomes imperative to have a strong online safety policy which gives clear picture of what is expected. It is also essential to connect this policy to other policies of the school to make it integral.
The Online Safety Policy of Eminence Private School aims to do ensure safe use of digital resources and technology.

Scope

This policy applies to all members of the school (including staff, students, parents, visitors) who will have access to and are users of school digital systems, on campus and/or remotely.

Review

Due to the ever-changing nature of digital technologies, the school shall review the Online Safety Policy quarterly and, if necessary, at other instances in response to any significant new developments in the use of the technologies, new threats to online safety, local regulations or incidents that may take place.

Roles and Responsibilities

The designated Online Safety Leader shall take the responsibility for any online safety issues and concerns and will be leading the Online safety group. There are certain roles and responsibilities laid down to ensure the implementation of this Policy **(Refer Schools Online Safety Group Terms of Reference).** Here are the responsibilities listed out for core members of the group:

Roles and Responsibilities of Senior Leaders (Principal and Parent Organization Representative)

- Evaluate, support and monitor the entire e-safety procedures and program of the school.
- Ensure that the online safety leader and group knows their responsibilities and adheres to the same.
- Ensure that the e-safety drive of the school is in line with the school development plan.
- Attend the online safety group meetings as ex officio members at least once a month.
- Meet the online safety leader once a week for updates and strategies on e-safety.
- Represent the school for seminars and meetings along with the online safety leader where the presence of the school leader(s) is deemed imperative.

Roles and Responsibilities of Online Safety Leader

- Provide leadership to the e-safety initiative of the school.
- Develop an e-safety culture in the school through a varied range of initiatives such as events, trainings, workshops, curriculum, and so on.
- Receive necessary training in e-safety, child protection and related topics and keeps updated about the latest developments on the same.
- Ensure that all members of the online safety group know their responsibilities and carries them out diligently.
- Have scheduled meetings with the group to discuss and address e-safety needs of the school.
- Convene emergency meetings in case of any incidents that require immediate attention and action.
- Ensure that all meetings have proper minuting and the same is filed for future reference.
- See to it that all departments systematically document all required matters related to e-safety such that they are easily accessible.
- Work with the school management, Principal, and HR Department to understand, develop and impart continuous training to the staff on online safety, acceptable use, child safety, anti-bullying and all matters related to e-safety.
- Ensure that e-safety policies are properly executed, reviewed and updated.
- See to the embedding of e-safety threads across policies of the school where they are relevant and essential.
- Develop, implement and monitor reporting strategies and systems to ensure that all e-safety safety incidents happening in and beyond school are addressed and followed up in a proper manner.
- Ensure that the e-safety curriculum is developed, imparted and updated as per plans.
- Work with the school team to plan and execute events and activities throughout every school year to promote e-safety.
- Follow up and receive appropriate MIS to ensure that all scheduled audits and monitoring of e-safety infrastructure is on track.
- Ensure that parents are informed and involved in the e-safety journey of the school.
- Liaise with government and non-government agencies to stay updated and also to report any incidents that require outside the school intervention / advice.
- Understand the statutory requirements of e-safety in UAE and ensure that the school systems are in compliance.
- Generate reports for the school management and/or leadership with regard to e-safety every 6 months and as per the demand.
- Represent the school for seminars and meetings on e-safety.
- Do adequate research, connect with various organizations and communities so that all the latest development in e-safety is known, and the same is integrated into the school where relevant.

Roles and Responsibilities of Online Safety Coordinator (IT Department)

- Ensure that the technical infrastructure is secure and is not open to misuse or malicious attack.
- See to it that the digital infrastructure meets required e-safety technical requirements and/or other relevant points from varied policies.
- Ensure that the school has proper age-appropriate filters in place, and these are monitored, reviewed and updated regularly.
- Take measures to ensure that users may only access the networks and devices through a properly enforced password and all such passwords are subject to change based on the requirements of the password policy of the school.
- Develop rubrics, structures and schedules for the monitoring, auditing and reviewing digital infrastructure and ensure that online safety leader and other relevant authorities are informed of any incidents or breaches.
- Ensure that all infrastructure related audits reports, incidents, breaches and the actions taken are properly documented,
- Stay connected to contracted and other agencies for digital infrastructural maintenance and the addressing of issues that cannot be solved from within the organization.
- Ensure that the online safety leader and group members are updated regarding any changes or improvements brought about in the system.
- Provide the online safety leader/ school management / school leadership half yearly reports on the digital infrastructure of the school.
- Be up to date with new developments with regard to digital infrastructure and e-safety so as to effectively advice the management and online safety group, update the systems and ensure there is no redundancy.

Roles and Responsibilities of Online Safety Assistant Coordinator (Staff representative)

- Work closely with the online safety leader in leading the committee and all roles and responsibilities.
- Follow up on the plans for the year and ensure that they are being carried out systematically.
- Advice the online safety leader of any deviations from plans or any breaches that need attention for the leader and the group.
- Guide the Student Online Safety Group in their activities.

Roles and Responsibilities of Child Protection Officer (School Counsellor)

- Take the lead along with online safety leader in ensuring in child protection.
- Immediately respond or step in when an online child safety incident occurs and work with the online safety leader, parents and students as required to address the same.
- Ensure that the evidence of intervention is documented.
- If appropriate, advise Online Safety Leader and school leadership for referral to external agencies.
- Be a part of the development, implementation and reviewing of the child protection policies of the school.
- Actively participate in the development of training modules for stakeholders on child protection, online behaviors and anti-bullying.
- Obtain training on handling various child protection and e-safety issues and stay updated on the same.

Roles and Responsibilities of Parent Representatives

- Assist the school in ensuring widespread parent participation for workshops and events of the school related to e-safety.
- Work with the school for the implementation of policies that pertain to students and parents.
- Encourage the implementation e-safety norms prescribed by the school for the home environment.
- Work with the school in the promotion of digital citizenship and responsible behavior.
- Alert the school in case of any issues that comes to the attention of the parent rep.
- Be a spokesperson for the school when it comes to e-safety.

Roles and Responsibilities of Student Representatives:

- Take the lead in the planning of events and activities for creating student awareness about e-safety.
- Actively participate and contribute to the digital citizenship program.
- Come up with ideas for improving student responsibility when it comes to the use of digital technology and discuss the same with the group to convert it into concrete plan of action.
- Contribute to e-safety policies via inputs shared through the Students Online safety group.
- Keep track of all records and minutes of their meeting with Students Online safety group and reporting it to the online safety leader.
- Report any trends or incidents that would have come to their purview to the online safety leader.
- Assist the teachers in the conduct of opinion polls, survey and campaigns.

Educating the Eminence Community

Educating School Leadership and Online Safety Group

Before the rest of the school community is made aware of the importance on online safety and safeguarding measures, it is essential for the school leadership as well as members of the Online Safety Group to be equipped. For this the school ensures that they obtain relevant training from outside accredited organizations as well as experts in the field on the same. The school management shall also see to it that the leadership and the group attend webinars and conferences (as deemed relevant) to keep themselves updates and bring about improvements in Eminence's e-safety initiative.

Educating students and parents

Ensuring that students and parents are well aware of the online safety norms and all related policies is part of the mission of the Eminence e-safety initiative. For this the school embeds e-safety into its year plan (reference e-safety year plan) and runs programs, events and workshops throughout the year. The programs have clearly set learning outcomes and built-in feedback and/or assessment systems that ensures that the outcomes are met with. In case there is a gap, follow up programs are done to bridge the same. Some initiatives to ensure awareness are:

- All relevant policies updated on the school's website.
- Induction program for parents and students on e-safety at the beginning of the academic year.
- Periodic posters, tips and articles sent to parents and students (age appropriate) on digital safety.
- Classroom activities and events that involve students so that they learn about e-safety hands on.

- Minimum of 3 student workshops every year.
- Minimum of two parental workshops in a year.
- Incorporating e-safety in other subjects where chapters enable the same.
- Introduce and run a PHSE curriculum that incorporates strands of e-safety.
- Ensure that students are given due classes on digital citizenship.
- Distribution of updated student handbooks to both parents and students at the beginning of every academic year.
- The important helpline numbers provided on the website.
- Oath taken by students at the beginning of every year on e-safety (reference e-Safety oath of the school).
- Acceptable usage agreement is signed by every parent on behalf of their wards when they join the school.
- Parents are explained the relevance of the Media Release Consent Form and they sign the same at the beginning of the academic year.
- Reminders sent to parents to read up and understand e-safety guidelines posted on website.
- Updates on policies and guidelines communicated to parents and students when such updates occur.
- School newsletter and blog which highlights e-safety as well.
- Student council active involvement in educating their peers about e-safety.

Educating Staff

Just like students and parents, it is very essential for all staff of Eminence to be aware of and be well equipped with online safety and all related policies. For this the following plans are put into action every year.

- Every new staff is inducted on e-safety norms.
- Refresher programs and workshops are provided to staff throughout the year at different pre-fixed intervals.
- Training on how to detect or look for signs of abuse and the system of alerting the required persons in case of a suspected case.
- Staff are required to take online safety e-courses so that they are equipped from outside accredited organizations on handling the same.
- Staff are assessed through online quizzes and MCQs on important e-safety norms. In case any staff fall below the 60 percent margin, the staff is given a one-on-one sitting by Online Safety Leader to equip that particular staff.
- Every staff signs the Acceptable Use Agreement when they join the organization.
- They also sign agreement on mobile devices – if provided by the school / BYOD as per the device ownership. (Reference Mobile device policy)
- Regular tips and updates are shared with staff on e-safety.
- The IT Department regularly send staff updates on how to increase the security of their system. They are also given alerts for antivirus update and password change.
- Awareness program is conducted regarding the school reporting systems for online incidents, child protection and other relevant areas as well as the sanctions connected with them. This helps them support each other, students and parents where needed.

Strategies for Managing Unacceptable Use

The school takes full responsibility for ensuring that the school digital infrastructure is safe and secure as is reasonably possible and that policies and procedures for ensuring e-safety are adhered to without fail. It shall also ensure that the relevant people named in the online safety group will be effective in carrying out their e-safety responsibilities. Other strategies that Eminence Private School shall take up to curb unacceptable usage are as below:

- The firewalls and filtering systems are set in place and are monitored closely by the IT Coordinator.
- Student centered events, programs and activities shall be conducted throughout the year.
- Regular trainings, workshops, quizzes and sessions shall be conducted for staff, students and parents to increase the awareness on online safety and responsible way of using the technology.
- Audit of the digital devices shall be conducted as per the checklist to ensure the safety and security of the device set by the IT department and reports are filed after the audit.
- Regular audit of the filtering system shall be conducted by the IT coordinator and all the reports and findings are given to the online safety leader in their regular online safety group meetings.
- School shall put into action the set sanctions for both staff and students for managing the unacceptable use of technology and all the actions are taken in accordance with the guidelines provided in the MoE student behavior policy.
- IT coordinator shall ensure that only school provided credentials are only used for logging into the school network and other school digital platforms.
- Clear reporting system shall be in place so that online incidents are handled as per the severity.
- Review of online incident reports every quarterly is conducted by the senior leadership team and the core members of Online Safety group.
- Based on overall review of e-safety in the school that happens every half year the management and school leadership shall decide on updating the policies and practices and bring into picture improvements.

Schools Sanctions

Separate sanctions (as mentioned in the Acceptable Use Policy) are in place for staff and students when there is breaches in what is deemed as acceptable.

Data Protection

As a school, Eminence is in possession of a lot of personal information of its staff and students. The **Data Protection Policy** of the school is put in place to protect such data and assure stakeholders of responsible handling of such data. Following guidelines are ensured while working with sensitive data:

- Users will respect the confidentiality and privacy of individuals whose records they access, observe ethical restrictions that apply to the information they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information.

- Employees are not allowed to take personal/sensitive data of any other person off campus (or to make unofficial copies). Sanctions will be applicable if such breach is revealed.
- Use such data only for the purpose for which access is provided.
- When printing or photocopying personal data, ensure that only authorized personnel will be able to access the same.
- Do not send personal information via email, instant message, chat or any unsecured file transfer unless it is encrypted.
- Backups of confidential data are always subject to the same restrictions as the original data.

The commitment of the school when collecting and using personal data is as below:

- Inform individuals why the information is being collected
- Inform individuals and gain consent when their information is to be shared with any entity other than the Ministry of Education or any Govt. agency where sharing of such information is legally allowed/required
- Ensure that information is not retained for longer than necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely.
- Breach of data protection policy shall be considered gravely and dealt with in accordance with the sanctions as mentioned in the policy (Reference Data Protection Policy).

Media Consent

Whenever a new student joins school at the time of admission parents shall sign a media release form after (Refer Appendix 1 at the end of the document) where the parent permit the school to use their wards images/works in school's social media sites, website as well as videos. Parents always have the option of refusing to sign the form wherein the school shall refrain from using that student's images.

Internet Access for Visitors and Guests

Visitors shall be provided with a separate controlled access to the School Wi-Fi, with limited access as set by the school. Once connected to the Eminence network, all visitors shall be required to strictly follow the security requirements of Eminence. This password for the same shall be changed every month in case of Front Desk guests. In case of other guests such as trainers, inspectors etc, the password would be changed once their usage during that visit is completed.

Monitoring and Intervention of Online Safety Incident

Eminence strives to build a culture of being digitally safe. For this it encourages pupils, staff and parents to engage with technology in a productive, and positive manner. At the same time, it is important to have a balance between allowing freedom to explore and use digital tools to their full potential and installing strong controls. In order to ensure this Eminence has a well-structured monitoring and intervention strategies.

Filters and Authorized Monitoring

- Through firewalls and filters the usage of the digital infrastructure is limited to what is considered acceptable by the school **(Reference: Acceptable Use Policy).**
- Internet access is filtered age appropriately and as per UAE norms.
- IT equipment shall be audited regularly (based on pre-fixed schedules) by the IT Coordinator
- Over and above regular digital devices audit, the school reserves the right to inspect any and all usage of technology devices, digital resources, and network infrastructure provided by the school as well as user owned devices if used on school network, with or without prior notice, in the case of a suspected malpractice/breach.
- Regular audit of password strength statistics shall be done and maintained by the IT coordinator. (Reference school password policy). Audit of sensitive data handled by HR, Accounts, and Registrar would be done by the IT coordinator with prior notice and in the presence of the respective department head to ensure the effective data handling and security of the system. Reports on such audits will be shared with respective department heads and corrective action designed by the department head and online safety leader where required.
- Alerts shall be set in case users accessing the blocked sites and repeated offenders shall be reported to the safety leader for further action.
- Incident reports and logs shall be shared with the online safety leader.

Process of Logging Online Incident Report

Following are the guidelines to be followed while logging any online incident report:

- Any material found by any member of the school community that is believed to be unlawful or against the guidelines set forth by the school shall be reported to the Online Safety group members based on the severity and based on the type of activity as mentioned in the Online Incident Report Flowchart.
- If the need arises the same shall be escalated to the school leadership team for appropriate action. A breach or suspected breach of this safe practice may result in the temporary or permanent withdrawal of School IT hardware, software or services from the offending individual. (Reference : Medium severity in Online Incident Flowchart)
- Any issue going beyond the high severity condition for both staff and students would be escalated to a third party or external agency after a joint decision with the school management. In case of a student, decision would be made in the presence of parent.
- All the online safety Incident report logs would be logged by the IT department and these logs **(Refer Appendix 2 at the end of the document)** would be regularly reviewed by the online safety leader and the Senior Leadership in their review meetings.
- The same process is maintained for the anonymous reporting as well keeping the confidentiality of the anonymity intact.

Reporting Mechanism

The reporting structure for online incidents is maintained looking into the severity of the act and escalation points (reference Online Incident Reporting Chart). School also provides students and staff to carry out anonymous reporting. Both types of reporting mechanism are carried in a similar manner.

Online Incident Reporting mechanism for Non – Anonymous cases

The online incidents are categorised into two for easier handling

1. Illegal activity/Content
2. Inappropriate activity/content

Based on the severity of the issue the reporting and handling mechanism is carried out as mentioned in the online incident reporting flow chart. The below table mentions the action that will be taken in case of such incidents in brief:

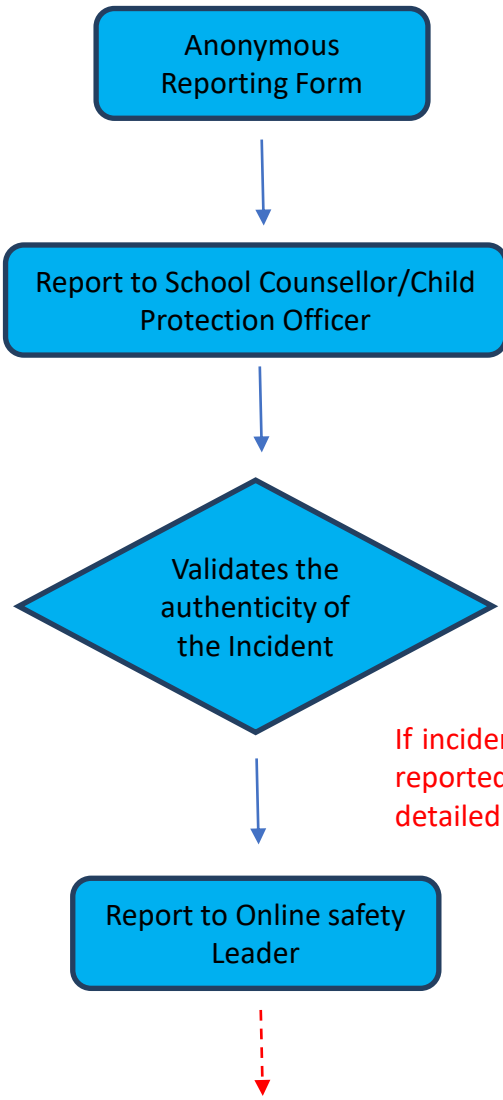
Severity	Staff	Action Plan	Student	Action Plan
Low	Reporting to Immediate head	Verbal warning	Reporting to School Counsellor/Teacher/ Online Safety coordinator	Verbal warning
Medium	Report to HR and Online Safety leader	Warning letter/memo – with suspension from online platform for few days	Report to parents and Online safety leader	Warning letter to parents with suspension from school for 2 days
High	Report to Senior leadership and management	Further recurrence of such incidents would result in immediate termination from job and Reporting to External agencies with all relevant evidences for further actions	Report to Senior leadership team and parents	Further recurrence of such incidents might result in expulsion from school and reporting to external agencies

Online Incident Reporting mechanism for Anonymous cases

Though at present the school will be using google forms for anonymous reporting, the school plans to use Whisper / bravely for the same soon in the near future.

Anonymous Reporting Protocol

If the incident reported by the anonymous person is validated as genuine, then the following reporting protocol follows as shown in the flowchart:



Emergency Contact Details for Reporting

School stakeholders can always approach the school directly or seek help from the following when there is an incident.

School Contact Details

Front Desk: 092220404
School Mobile Number: 0547999720

Mail ids: Online Safety Leader ops.manager@eminenceschool.org
School Counsellor counsellor@eminenceschool.org

Other useful helpline numbers or sites to report incidents in UAE

Call 04-217666/116111 or email to: cpu@moe.gov.ae to report any child abuse.
Call 999 for any emergencies (Police).
Call 8002626 to report any kind of cybercrime.

One can report cybercrimes online through the following channels as well

The eCrime website
Dubai Police's website
the 'My Safe Society' app launched by the UAE's federal Public prosecution (the app is available on iTunes or Google Play)

Guidelines of MoE on Online Safety

The School ensures to follow all the guidelines laid by MoE and incorporate into the system for the well-being and security of the whole school community. Guidelines are followed in Child Protection Policy, Behaviour Policy, as well as in Anti-bullying policies. The sanctions set forth by the Ministry is also adhered to.

Eminence is aware of MoE's child protection unit specially designed to implement the mechanisms and measures of child protection in educational institutions as stipulated in the Federal Law No. 3 for 2016 and its executive regulations.

Ministry of Education (MoE) has launched a 'Child Protection Unit' initiative for the benefit of students of government and private schools across the UAE. The initiative is aimed at protecting children from all forms of harm, negligence and abuse which they may experience at school or home and maintaining their safety with regard to their physical, psychological and educational aspects.

Cross References

The following policies are also linked to the School's online safety practice.

Acceptable Use Policy
MOE Student behavior Management – Distance learning Policy
Mobile Device Policy
Cyberbullying Policy
PSHE Policy
Child Protection Policy
Online Behavior Policy (Staff and Student)
Communication Policy
Online Incident Flowchart
Data Protection Policy
Data Backup Policy

Resources link:

Home | eSafe (esafesociety.org)
eCrime (dubaipolice.gov.ae)
How to Report a Cybercrime in the UAE (onlinesense.org)
الصفحة الرئيسية(pp.gov.ae)