IDEAL ENGLISH SCHOOL

RAK

ONLINE SAFETY POLICY

2022 – 2023

Strand 2

RESPONSIBILITIES

Aspect 1: Online Safety Leader

Aspect 2: Online Safety Group

POLICY	ONLINE SAFETY POLICY
Status	Implemented
Focus	School's Online safety Norms
Responsibility	School Leadership & Online Safety Group
Applicability	School Community
Prepared By	SLT Team
Date of Review	January 2020
Next Review	January 2022

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. 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 Ideal English 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, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

1. The School is committed to promoting and safeguarding the welfare of all students and an effective online safety is of paramount importance.
2. To apply the principle and culture of reinforcement, encouragement and permanent care to the educational setup, stakeholders and the wider community to reduce behavioural offences inside and outside the walls of the school with the best possible educational means through online safety and promoting values of digital citizenship.
3. Offences and behaviours in the virtual school will be in line with that defines the rules, standards and procedures to be invoked or deal with the students' behaviour in way that it ensures compliance with the school values and systems in line with the ministry online behaviour guidelines for the changing and emerging conditions.

THE AIMS OF THE SCHOOL'S ONLINE SAFETY STRATEGY ARE THREEFOLD:

To protect the whole School community from illegal, inappropriate and harmful content or contact.

1. To educate the whole School community about their access to and use of technology; and
2. To establish effective mechanisms to identify, intervene and escalate incidents where appropriate.
3. In considering the scope of the School's online safety strategy, the School will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information including communications technology (collectively referred to in this policy as Technology).
4. This policy applies to all members of the School community, including staff, students, parents and visitors, who have access to the School's Technology whether on or off, School premises, or otherwise use Technology in a way which affects the welfare of other students or any member of the School community or where the culture or reputation of the School is put at risk.
5. The following policies, procedures and resource materials are also relevant to the School's online safety practices:
   - ❖ Acceptable Use Policy for Students
   - ❖ E-learning Cyber Safety policy
   - ❖ Digital well-being policy
   - ❖ MOE Student behaviour Management – Distance Learning
   - ❖ Computing Policy
   - ❖ Induction Policy
   - ❖ Acceptable Use Policy for staff
   - ❖ Data Protection Policy
   - ❖ ICT Firewall Policy
   - ❖ Mobile Technologies Policy
   - ❖ Password policy
   - ❖ Child protection policy
   - ❖ Risk Management Policy
   - ❖ Password Policy

This is a whole School policy and applies to Ideal English School , RAK

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 .

THE GOVERNING BODY : Dr. Prasanna Bhaskar

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- ❖ Regular meetings with the E-Safety Coordinator
- ❖ Regular monitoring of e-safety incident logs
- ❖ Regular monitoring of filtering / change control logs
- ❖ Regular updates on the monitoring of the filtering of web sites
- ❖ Reporting to relevant Governors / Board / Committee / meeting
- ❖ Supporting the head teacher (or designated member of staff) in developing an appropriate strategy and plan for dealing with the media should serious incidents occur
- ❖ To ensure that all staff are aware of the procedures that need to be followed in the event of an E- Safeguarding incident.
- ❖ To read, understand and help promote the school's E -Safeguarding policies and guidance.

  - ❖ The Governing Body has overall responsibility for ensuring safeguarding arrangements within the School, including the School's approach to online safety and the use of technology and provide access to appropriate resource required by the IT team and the Principal in safeguarding the online safety of students within the School
  - ❖ The Governing Body is required to ensure that all those with leadership and management responsibilities at the School actively promote the well-being of students. The adoption of this policy is part of the Governing Body's response to this duty.

ONLINE SAFETY LEADER : **Mrs. Betsy .M. Miranda**

- ❖ 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.
- ❖ 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.

E SAFETY COMMITTEE: **Mrs. Shyla, Mrs. Haseen Taj, Mrs Jenila ,Mrs. Shazalia**

- ❖ Representatives are responsible for the implementation of the E safety Policy and for the reviewing the effectiveness
- ❖ Providing training and advice for teachers students staff & Parents
- ❖ To ensure that all new staff and pupils are aware of its content and have acknowledged appropriate AUP and attend regular meetings with E safety leader
- ❖ Ensure that all staff is aware of procedures that need to be followed in the event of and E safety instant taking place and maintaining and E safety instant log book.
- ❖ Regular Updates on the monitoring of safety incidents and reporting to the leader
- ❖ They have an up to date awareness of E safety matters and of the current school e safety Policy and practices.

ROLES AND RESPONSIBILITIES OF CHILD PROTECTION OFFICER

(SCHOOL COUNSELLOR) : Mrs. Reena M.R

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**.**

Special educational needs co -ordinators may need to work closely with the child protection liaison officer within their school. Suggested responsibilities for special educational needs co-ordinators include:

✓ developing and maintaining knowledge of internet safety issues, particularly with regard to how they might affect children and young people

✓ developing and maintaining additional policies and internet safety materials, in conjunction with the internet safety co-ordinator and the school's internet safety team, tailored to the special educational needs of pupils

✓ liaising with parents of pupils with special educational needs to ensure that they are aware of the internet safety issues their children may encounter outside school, and the ways in which they might support them

✓ co-operating with the child protection liaison officer, as necessary liaising with other individuals and organisations, as appropriate, to ensure that those pupils being educated away from school premises still benefit from a safe ICT learning environment

The School Counsellor with lead responsibility for safeguarding and child protection along with the Online Safety Leader and Designated Safeguarding Leads.

❖ All incidents will be reported accordingly to the Principal and Designated Safeguarding Leads.
❖ Immediately respond when safety incident occurs
❖ Conducting audit of the online safety incidents, maintain logs and monitoring.
❖ Assessing the problem
❖ Determining consequences in accordance with school policies.
❖ Escalate to the higher authorities.
❖ Provide the necessary safeguards and support for all pupils involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support
❖ Inform parents, if appropriate, about the incident and how it is being managed
❖ If appropriate, advise Online Safety Leader for referral to external agencies.

THE KEY RESPONSIBILITIES OF PARENTS AND CARERS:

✓ Reading the school/setting Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.

✓ Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.

✓ Role modelling safe and appropriate uses of technology and social media.

✓ Identifying changes in behaviour that could indicate that their child is at risk of harm online.

✓ Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.

✓ Contributing to the development of the school/setting online safety policies.

✓ Using school systems, such as learning platforms, and other network resources, safely and appropriately.

✓ Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

THE KEY RESPONSIBILITIES OF STUDENTS (PRIMARY LEVEL)

✓ Contributing to the development of online safety policies.

✓ Reading the school/setting Acceptable Use Policies (AUPs) and adhering to them.

✓ Respecting the feelings and rights of others both on and offline.

✓ Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.

✓ Taking responsibility for keeping themselves and others safe online.

✓ Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

✓ Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

ROLES AND RESPONSIBILITIES OF DATA PROTECTION OFFICER

DATA PROTECTION OFFICER

The managed service provider is responsible for helping the school to ensure that it meets the E-Safety technical requirements outlined by aqdar.

The managed service provides a number of tools to schools including, Smart cache servers, Secures (optional), Safety Net Universal, which are designed to help schools keep users safe when online in school Update a range of Acceptable Use Policies and any relevant Local Authority E-Safety policy and guidance. These can be accessed either on micro soft team or via the E-Safety interest space on the portal

- ❖ 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.
- ❖ The school's policy on web filtering is applied and updated on a regular basis.
- ❖ Developing a parental awareness programme, in consultation with the parent–teacher association, as appropriate.
- ❖ Maintaining a log of all incidents relating to internet safety in school.
- ❖ Meeting regularly with the head teacher to discuss internet safety issues and review progress.
- ❖ Liaising with outside agencies, which may include the local schools, city learning centre, or national agencies, as appropriate
- ❖ To maintain a professional level of conduct in your personal use of technology at all times.
- ❖ To support the school in providing a safe technical infrastructure to support learning and teaching.
- ❖ To ensure that access to the school network is only through an authorized, restricted mechanism.
- ❖ To ensure that provision exists for misuse detection and malicious attack.
- ❖ To take responsibility for the security of the school ICT system.
- ❖ To liaise with the local authority and other appropriate people and organizations on technical issues.

ONLINE SAFETY COMPUTING COORDINATOR : Mrs. Gomathi & Mrs. Shalini

The IT Manager as E- Safety Coordinator is responsible for ensuring that:

(a) The School's Technology infrastructure is secure and, so far as is possible, is not open to misuse or malicious attack.

(b) The user may only use the School's Technology if they are properly authenticated and authorized.

(c) The School has an effective filtering policy in place and that it is applied and updated on a regular basis.

(d) The risks of students and staff circumventing the safeguards put in place by the School are minimized;

(e) The use of the School's Technology is regularly monitored to ensure compliance with this policy and that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation; and

(f) Monitoring software and systems are kept up to date to allow the ICT team to monitor the use of email and the internet over the School's network and maintain logs of such usage.

- ❖ The IT Manager will provide details on request outlining the current technical provision and safeguards in place to filter and monitor inappropriate content and to alert the School to safeguarding issues.

- ❖ The IT Manager will report regularly to the SLT on the operation of the School's Technology. If the IT Manager has concerns about the functionality, effectiveness, suitability or use of Technology within the School, s/he will escalate those concerns promptly to the appropriate members(s) of the School's Senior Leadership Team (SLT).

- ❖ The IT Manager is responsible for maintaining the Technology Incident Log and bringing any matters of safeguarding concern to the attention of the Designated Safeguarding Lead in accordance with the School's Child Protection & Safeguarding Policy and Procedures.

- ❖ Leads the e-safety committee.

- ❖ Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents .

- ❖ Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place .

- ❖ Provides training and advice for staff .

- ❖ Liaises with the KHDA / relevant body

- ❖ Liaises with school technical staff

- ❖ Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments

- ❖ Meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs

- ❖ Attends relevant meeting / committee of Governors

- ❖ Reports regularly to Senior Leadership Team.

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

RESPONSIBILITIES OF PARENTS / CARERS

The role of parents in ensuring that students understand how to stay safe when using Technology is crucial. The School expects parents to promote safe practice when using Technology and to:

- ❖ Support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures;
- ❖ Talk to their child / children to understand the ways in which they are using the internet, social media and their mobile devices and promote digital citizenship and responsible behaviour;
- ❖ Encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support
- ❖ Participate in the Surveys conducted by the school and MOE which helps the school in informing appropriate intervention to be taken.
- ❖ Contribute to the school policies, to be read, understood, acknowledge and provide appropriate feed back .
- ❖ If parents have any concerns or require any information about online safety, they should contact the DESIGNATED SAFEGUARDING LEAD.
- ❖ 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 spoke person for the school when it comes to e-safety.

ICT TECHNICAL SUPPORT : MR.ZUBAIR AHMEDH

The Director of Digital & IT is responsible for ensuring:

- ❖ That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- ❖ That the school meets required e-safety technical requirements and any KHDA / other relevant body E-Safety Policy / Guidance that may apply.
- ❖ That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- ❖ The filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- ❖ That they keep up to date with e-safety technical information in order to effectively carry out their e safety role and to inform and update others as relevant
- ❖ That the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head of Year / Principal / Senior Leader; E-Safety Coordinator

CURRICULUM LEAD : Mrs. Shyla, Mrs Kavitha , & Mrs Jenila

The Head teacher is responsible for ensuring the safety.

- ❖ The schools is responsible for reporting security incidents as outlined in the schools Information Security The day to day responsibility for E-Safety will be delegated to all staff who work with pupils including the SLT.
- ❖ The Headteacher /SLT are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable cooperation to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.
- ❖ They are also responsible for ensuring that pupils and students are taught how to use ICT tools such as the internet, email and social networking sites, safely and appropriately
- ❖ The Headteacher / SLT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- ❖ The Headteacher and another member of the SLT should be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff
- ❖ The SLT will receive regular monitoring reports from the E-Safety Co-Ordinator / Officer
- ❖ The Head teacher is responsible for ensuring that parents and carers, when given access to data and information relating to their child/children via the learning platform, have adequate

information and guidance relating to the safe and appropriate use of this on line facility-(The Information Security Policy contains detailed guidance)

E-SAFETY COORDINATOR : Mrs. Radhika & Mrs. Shilba Rajana

Leads the e-safety committee

- ❖ Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ❖ Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- ❖ Provides training and advice for staff
- ❖ Liaises with the KHDA / relevant body
- ❖ Liaises with school technical staff
- ❖ Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- ❖ Meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- ❖ Attends relevant meeting / committee of Governors
- ❖ Reports regularly to Senior Leadership Team.

RESPONSIBILITIES OF STUDENTS / PUPILS

- ❖ To read, understand and adhere to the school pupil Acceptable Use Policy.
- ❖ To help and support the school in the creation of eSafeguarding policies and practices and to adhere to any policies and practices the school creates.
- ❖ To know and understand school policies on the use of mobile phones, digital cameras and handheld devices.
- ❖ To know and understand school policies on the taking and use of mobile phones.
- ❖ To know and understand school policies regarding cyberbullying.
- ❖ To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home.
- ❖ To be fully aware of research skills and of legal issues relating to electronic content such as copyright laws.

❖ To take responsibility for each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used outside school.

❖ To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.

❖ To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to.

❖ To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within school.

❖ To discuss eSafeguarding issues with family and friends in an open and honest way.

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.

❖ The School Counsellor with lead responsibility for safeguarding and child protection along with the Online Safety Leader and Designated Safeguarding Leads.

❖ All incidents will be reported accordingly to the Principal and Designated Safeguarding Leads.

❖ Immediately respond when safety incident occurs

❖ Conducting audit of the online safety incidents, maintain logs and monitoring.

❖ Assessing the problem

❖ Determining consequences in accordance with school policies.

❖ Escalate to the higher authorities.

- ❖ Provide the necessary safeguards and support for all pupils involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support
- ❖ Inform parents, if appropriate, about the incident and how it is being managed
- ❖ If appropriate, advise Online Safety Leader for referral to external agencies.

STUDENT DIGITAL LEADERS AND DIGITAL MONITORS:
Miss Varshini ,Master Nafeez,Miss Malavika

- ❖ An essential part of the school's Online Safety Group is the Student Digital Leaders and the extended online safety group consisting of the Digital Monitors.

  a) The Digital Leaders are a part of the School's Student Council and has representation from all age-groups and phases.

  b) They should act as the digital ambassadors or role-models and ideal digital citizens amongst their peers by adopting safe internet practices and digital citizenship.

  c) The Digital Leaders should take part in the Online Safety Group meetings and contribute through giving feedback on the Online Safety Policy and all other related policies.

  d) They should assist in the Online Safety Education programme assisting the Counsellor and Heads of Sections during the training programmes on Digital Citizenship and Online Safety Education programme.

  e) Help the Senior Leaders in evaluating the online safety programme through their feedback.

  f) Conduct weekly meetings with the extended Online Safety Group consisting of 70 Digital Monitors representing each Class.

  g) Gather feedback and spread awareness on online safety and reporting online safety incidents through the Digital Monitors.

  h) Assists the Child protection Officer in terms of safeguarding by reporting incidents and cascading information related to online safety and cyberbullying.

  i) Contribute towards the creation of digital content and/or share their expertise in training their peers to create them.

  j) Contribute to awareness drives through newsletters, interactive sessions and posters.

  k) Support other students in their understanding of online safety, digital safety, digital security, digital identity, digital communication and digital literacy.

EDUCATING THE EMINENCE COMMUNITY

STUDENTS :

The safe use of Technology is integral to all School's policies and routines.Students are educated in an age-appropriate manner about the importance of safe and responsible use of Technology, including the internet, social media and mobile electronic devices.

Technology is included in the educational programmes followed in the EYFS in the following ways:

(a) children are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment;

(b) children are enabled to explore and play with a wide range of media and materials provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, movement, dance, role-play, and design and technology; and

(c) children are guided to recognise that a range of technology is used in places such as homes and Schools and encouraged to select and use technology for particular purposes.

The School's Acceptable Use of ICT Policy, BYOD policy, Online behaviour policy for Students sets out the School rules about the use Technology including internet, email, social media and mobile electronic devices, helping students to protect themselves and others when using Technology. Students are reminded of the importance of this policy on a regular basis.

STAFF

The School provides training on the safe use of Technology to staff so that they are aware of how to protect students and themselves from the risks of using Technology and to deal appropriately with incidents involving the use of Technology when they occur.

Are Responsible for ensuring that :

- They have an upto date awareness of e safety matters and of the current school e safety policy & Practises.
- They encourage pupils to develop good habits when using ICT to keep themselves safe.
- They have read understood and signed the school staff AUP

- The report any suspected misuse or problem to the E safety Co-ordinator /Head Teacher /Senoir leader /Class teacher for investigation /action/sanction.

- Digital Communication with students /pupils (email,Virtual learning environment /Voice) should be on a professional level and only carried out using official school systems

- E safety issues are embedded in all aspects of curriculum and other school activities

- Students/pupils understand and follow the school e safety and AUP

- Students /Pupil have a good understanding of research skills and need to avoid plagiarism and uphold copyright regulations.

- In lessons where internet use is preplanned ,student/pupil should be guided to sites checked as suitable for their use that processes are in place for dealing with suitable for their use and that processes are in place for dealing with suitable material that found in internet searches .They include the teaching of e safety in their lessons .

PARENTS

We offer the opportunity for parents to attend School based sessions on online safety on a regular basis. Information is available to parents via the school learning portal.

Training and awareness sessions will also be conducted in association with the Parent Advisory Board.

Parents are encouraged to read the Acceptable Use Policy for Students with their children to ensure that it is fully understood.

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:

2. 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:

3. Anonymous Reporting Form Report to School Counsellor/Child Protection Officer Validates the authenticity of the Incident Report to Online safety Leader If incident is validated as authentic, it will be reported to the online safety leader with detailed evidences of the incident Further actions are taken as based on the online incident flowchart for non-anonymous case 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 : **+971509312500**

ONLINE SAFETY LEADER : **+971566644829**

SCHOOL COUNSELLOR : **+971503463091**

MAIL IDS:

ONLINE SAFETY LEADER : Betsy@iesrak.com

SCHOOL COUNSELLOR : reena@iesrak.com

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.

. Where to go for help

If your child is affected by something they've seen or experience online there are lots of places to go for more help and advice. Here are some recommended organisations to contact:

ORGANISATIONS

Child Protection Center Hotline #11611, Ministry of Interior, UAE

Aman Centre for Women and Children through RAK Police: 07-2356666 or email: CPU@moe.gov.ae

REPORTING INCIDENTS ONLINE IS SIMPLE

JUST VISIT THE SCHOOL WEBSITE OR PORTAL