EMINENCE PRIVATE SCHOOL

مدرسة أيمينينس الخاصة

Acceptable Use Policy

Version 4.0

POLICY	ACCEPTABLE USE POLICY
STATUS	Implemented
FOCUS	Expectations and sanctions when it comes to digital infrastructure usage
RESPONSIBILITY	Principal and Online Safety Group
APPLICABILITY	School Community
DATE OF REVIEW	FIRST REVIEW: September 2020 SECOND REVIEW :February 2021 THIRD REVIEW: March 2022 FOURTH REVIEW: March 2023 NEXT REVIEW: June 2024

Policy Objective

This Acceptable Use Policy outlines the guidelines and behaviors that all users are expected to follow when using digital devices, the school internet, and the school provided IDs and software access. In the school, a balance is required between setting rules and allowing the liberty to explore, connect and experiment while advocating responsible use. This policy educates the users of their rights and duties and enable the users to leverage digital ecosystems with confidence for their online experience. This policy also protects the interests and safety of the whole school community.

Rationale

In today's world it is impossible to provide education without the use of digital technologies and infrastructure. Staff and students have access to various devices and software that enable them to carry out their tasks more effectively. This makes it imperative that some guidelines are set forth such that ethical and safety standards are maintained. The acceptable use policy informs users about the provisions that have been made to ensure the ethical and safe use of digital infrastructure and devices.

Roles and Responsibilities

The Principal and the Online Safety Group (Reference in Online Safety Policy) is responsible to ensure that the policy is adhered to by all concerned. At the beginning of every academic year an Acceptable Use Agreement form (Reference attached at the end of this document) would be sent to all Staff and Students (to be signed by Parents).

Scope

This policy applies to all the stakeholders in the school community. The policy shall be reviewed annually and modified as per need.

Monitoring and Privacy

Access to information technology through Eminence private School is a privilege, not a right. It is expected that staff and students comply with the e-safety rules of the school. 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, with or without prior notice, in the case of a suspected malpractice.

Guidelines

Eminence Private School considers the following activities as **acceptable** when using school equipment, software, networks or technologies.

General Guidelines for Staff and Students

- Using the school's resources and technologies only for school related purposes.
- Using only school assigned email accounts for online communication.
- Keeping passwords and personal information secure.
- Observing all school Internet filters and posted network security practices.
- Respect the rights, beliefs and viewpoints of others.
- Following the same standards of behavior online as would be expected to follow in real life
- Reporting security risks or violations to an authorized personal or IT In-charge. In case of students such reporting can be done to a teacher.
- Disclose to an authorized personal or the IT In-charge any messages that users receive that are inappropriate or disturbing. In case of students such reporting can be done to a teacher.
- Protecting data, networks, or other digital resources of the school.
- Following copyright laws.
- Citing sources when using others' work.
- Communicating only in ways that are kind and respectful.
- Ensuring that any social networking sites /blogs that are created or actively been contributed are not confused with ones' professional/student role.
- Ensuring that all the data, documents saved, accessed and deleted are in conformance with EPS network protocols.
- Being aware of the fact that unauthorised individuals are not allowed to access ones' school email or other EPS system.

The school believes that the activities referred to below would be **inappropriate/unacceptable** and that users should not engage in these activities when using school equipment, software, networks or technologies.

- Visiting internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:
    - Pornographic, obscene, vulgar and/or indecent materials
    - Promotion of any kind of discrimination
    - Promotion of racial or religious hatred
    - Promotion of political views
    - Cyber bullying
    - Any other information which may be offensive to colleagues or classmates, or breaches the integrity of the school or brings the school into disrepute.
- Using unauthorized video broadcasting or sharing of files.
- Using school systems to run a private business

- Saving inappropriate files to any part of the school issued system, including but not limited to:
  - Music files
  - Movies
  - Video games of all types
  - Offensive images, videos or files
  - Programs which can be used for malicious purposes
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Eminence Private School.
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- "Hacking" and other illegal activities in attempt to gain unauthorized access to restricted files, other devices or computer systems.
- Revealing or publicizing confidential or proprietary information (like financial / personal information, databases, computer / network access codes and passwords).
- Creating or propagating computer viruses or other harmful files.
- Removing or relocating school-owned technology resources requires prior authorization from the IT coordinator.
- Carrying out sustained or instantaneous high-volume network traffic (downloading / uploading heavy files) that causes network congestion and hinders others in their use of the internet
- Online gaming and/or gambling
- Online shopping or any kind of e-commerce
- Streaming movies of music online
- Spamming, sending out chain letters, or other mass unsolicited mailings.
- Use of personal social media accounts or sites.
- Connect to any computer or devices including a USB flash drive to the network/ Internet that does not have up to date antivirus software or school recommended firewall system.
- Use of personal digital cameras or camera phones for taking and transferring images of students or staff without permission and storing images at home without permission.
- Accessing and trying to change any other person's username, password, files or data.
- Insulting any peer or members of school on social media with defaming content and provocative comments.

Parent specific guidelines

- Ensuring that their wards G-Suite is uploaded with documents related only with educational or learning purpose.
- Ensuring that their ward do not misbehave or cause disturbance during online classes.
- Seeking support from school in case of any misuse or online incidents happen.
- Changing the password of the software/email allotted by the school every time mail or message to do the same comes from the IT department of the school.

Sanctions for Unacceptable Use

The school has set certain guidelines (based on MoE student behaviour policy) and reporting protocols on unacceptable use of technology and digital infrastructure. Sanctions are present for both staff and students. Actions are taken based on the severity of the incident.

For Staff: Sanctions attached at the end of this document
For Students: Sanctions attached at the end of this document
The School has aligned unacceptable use with MoE's behavioural policy as below:

ALIGNMENT OF SCHOOL's UNACCEPTABLE USE TO MOE's BEHAVIOURAL POLICY	
MOE Behavioural Policy	**School's Unacceptable Use**
• Verbal abuse or insulting students, staff or school guests. • Attempting to defame or abuse school mates • Cyberbullying • Bullying of various kinds and forms. • Incitement to fight, threaten or intimidate classmates. • Sexual harassment within the school • Physical assault on peers or school workers	• Cyberbullying • "Hacking" and other illegal activities in attempt to gain unauthorized access to restricted files, other devices or computer systems.
• Acquisition, possession, display and promotion of unauthorized physical media or electronic materials in violation of values, morals, etiquette and public order	• Using unauthorized video broadcasting or sharing files. • Creating or propogating computer viruses or other harmful files.
• Misuse of electronic devices during the period including electronic games and headphones in the class.	• Online gaming, online shopping, streaming movies of music online, and sending out chain letter, use of personal social media account.
• Misusing any means of communication.	• Using school system to run a private business
• Photocopying, publishing and circulating images of school personnel and school students without their permission.	• Use of personal cameras for taking photos images of students/staff without their permission.
• Defaming and insulting peers or school staff on social media	• Insulting any peer or members of school on social media with defaming content and provocative comments.
• Insulting heavenly religions, or provoking anything that causes sectarian strife in school • Broadcasting or promoting extremist, expiatory or atheistic ideas and beliefs against the social and political policies of society	• Promotion of racial or religious hatred • Promotion of any kind of discrimination • Promotion of political views

Formats

Acceptable Use Agreement
Acceptable Use Agreement for Staff (Appendix 1)
Acceptable Use Agreement for Students (to be signed by Parents) (Appendix 2)

Cross Reference

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

Online Safety Policy
MOE Student behavior Management – Distance learning Policy

Resource link

_Acceptable Use Policies – A Necessity for any Business – Olaf Solutions – Your Partner in Business

SANCTIONS FOR STAFF ON UNACCEPTABLE USE

	Low severity					Medium Severity				High Severity			
Incident Details	Reporting to Immediate Head/Coordinator	Reporting to School Counsellor	Reporting to Online Safety Coordinator/IT coordinator	Reporting to Online Safety Leader/Vice Principal	First Action Plan - Verbal Warning or memo	Reporting to HR	Reporting to Principal/Chairperson	Second Level Plan- written warning letter by the principal	Suspension from job for 2 days	If repeating, Suspension from job more until further notice	Joint decision by School Leadership, Online Safety group and parents	Immediate termination from job and HR submitting a copy of all memos and letters to the concerned authority	Reporting to External Agency/Police
Using unauthorized video for broadcasting or sharing of files	●	●	●	●	●	●							
Using School Systems to run a private business	●	●	●	●	●	●	●	●		●			
Saving inappropriate files to any part of the school issued system	●		●		●	●							
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school	●		●	●	●	●							
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties	●		●	●	●	●		●					

SANCTIONS FOR STAFF ON UNACCEPTABLE USE

	Low severity					Medium Severity				High Severity			
Incident Details	Reporting to Immediate Head/Coordinator	Reporting to School Counsellor	Reporting to Online Safety Coordinator/IT coordinator	Reporting to Online Safety Leader/Vice Principal	First Action Plan - Verbal Warning or memo	Reporting to HR	Reporting to Principal/Chairperson	Second Level Plan- written warning letter by the principal	Suspension from job for 2 days	If repeating, Suspension from job more until further notice	Joint decision by School Leadership, Online Safety group and parents	Immediate termination from job and HR submitting a copy of all memos and letters to the concerned authority	Reporting to External Agency/Police
Hacking and other illegal activities in attempt to gain unauthorized access to restricted files, other devices or computed systems	●	●	●	●		●	●		●	●			
Online gaming/Gambling Not Recommended for educational Purposes	●		●	●	●	●		●		●			
Online Shopping for ecommerce with school credentials	●		●	●	●	●							
Streaming movies with music online	●		●		●	●							

SANCTIONS FOR STAFF ON UNACCEPTABLE USE

Incident Details	Low severity					Medium Severity				High Severity			
	Reporting to Immediate Head/Coordinator	Reporting to School Counsellor	Reporting to Online Safety Coordinator/IT coordinator	Reporting to Online Safety Leader/Vice Principal	First Action Plan - Verbal Warning or memo	Reporting to HR	Reporting to Principal/Chairperson	Second Level Plan- written warning letter by the principal	Suspension from job for 2 days	If repeating, Suspension from job more until further notice	Joint decision by School Leadership, Online Safety group and parents	Immediate termination from job and HR submitting a copy of all memos and letters to the concerned authority	Reporting to External Agency/Police
Spamming, sending out chain letters or other mass unsolicited mailings	●	●	●	●	●	●		●					
Use of Personal social media accounts(not permitted by IT) during school hours	●		●	●	●	●							
Trying to connect devices like USB not updated with proper Antivirus to school devices or network	●		●	●	●								
Use of personal digital cameras for capturing images of students/staff and storing images without permission	●	●		●		●	●	●		●			
Accessing and trying to change any other colleagues or student's username, password, files or data	●		●	●		●		●		●			

SANCTIONS FOR STAFF ON UNACCEPTABLE USE

	Low severity					Medium Severity				High Severity			
Incident Details	Reporting to Immediate Head/Coordinator	Reporting to School Counsellor	Reporting to Online Safety Coordinator/IT coordinator	Reporting to Online Safety Leader/Vice Principal	First Action Plan - Verbal Warning or memo	Reporting to HR	Reporting to Principal/Chairperson	Second Level Plan- written warning letter by the principal	Suspension from job for 2 days	If repeating, Suspension from job more until further notice	Joint decision by School Leadership, Online Safety group and parents	Immediate termination from job and HR submitting a copy of all memos and letters to the concerned authority	Reporting to External Agency/Police
Revealing or publicizing confidential school credentials to third person	●		●	●	●	●		●					
Trying to remove school provided technology resources	●		●	●	●	●		●					
Visiting internet sites that are offensive and trying to post or communicate with staff or students	●	●	●	●	●	●	●			●			
Indulging in Cyberbullying activities	●	●	●	●		●	●				●	●	●
Promoting any kind of discrimination or racism in online groups	●	●	●	●		●	●				●	●	●

SANCTIONS FOR STAFF ON UNACCEPTABLE USE													
	Low severity					Medium Severity				High Severity			
Incident Details	Reporting to Immediate Head/Coordinator	Reporting to School Counsellor	Reporting to Online Safety Coordinator/IT coordinator	Reporting to Online Safety Leader/Vice Principal	First Action Plan - Verbal Warning or memo	Reporting to HR	Reporting to Principal/Chairperson	Second Level Plan- written warning letter by the principal	Suspension from job for 2 days	If repeating, Suspension from job more until further notice	Joint decision by School Leadership, Online Safety group and parents	Immediate termination from job and HR submitting a copy of all memos and letters to the concerned authority	Reporting to External Agency/Police
Using unauthorised video for broadcasting or sharing of files	●	●	●	●	●	●							
Using School Systems to run a private business	●	●	●	●	●	●	●	●		●			
Saving inappropriate files to any part of the school issued system	●		●		●	●							
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school	●		●	●	●	●							
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties	●		●	●	●	●		●					

SANCTIONS FOR STAFF ON UNACCEPTABLE USE

	Low severity					Medium Severity				High Severity			
Incident Details	Reporting to Immediate Head/Coordinator	Reporting to School Counsellor	Reporting to Online Safety Coordinator/IT coordinator	Reporting to Online Safety Leader/Vice Principal	First Action Plan - Verbal Warning or memo	Reporting to HR	Reporting to Principal/Chairperson	Second Level Plan- written warning letter by the principal	Suspension from job for 2 days	If repeating, Suspension from job more until further notice	Joint decision by School Leadership, Online Safety group and parents	Immediate termination from job and HR submitting a copy of all memos and letters to the concerned authority	Reporting to External Agency/Police
Hacking and other illegal activities in attempt to gain unauthorized access to restricted files, other devices or computed systems	●	●	●	●		●	●		●	●			
Online gaming/Gambling Not Recommended for educational Purposes	●		●	●	●	●		●		●			
Online Shopping for ecommerce with school credentials	●		●	●	●	●							
Streaming movies with music online	●		●		●	●							
Spamming, sending out chain letters or other mass unsolicited mailings	●	●	●	●	●	●		●					

SANCTIONS FOR STAFF ON UNACCEPTABLE USE

	Low severity					Medium Severity				High Severity			
Incident Details	Reporting to Immediate Head/Coordinator	Reporting to School Counsellor	Reporting to Online Safety Coordinator/IT coordinator	Reporting to Online Safety Leader/Vice Principal	First Action Plan - Verbal Warning or memo	Reporting to HR	Reporting to Principal/Chairperson	Second Level Plan- written warning letter by the principal	Suspension from job for 2 days	If repeating, Suspension from job more until further notice	Joint decision by School Leadership, Online Safety group and parents	Immediate termination from job and HR submitting a copy of all memos and letters to the concerned authority	Reporting to External Agency/Police
Use of Personal social media accounts during school hours	●		●	●	●	●							
Trying to connect devices like USB not updated with proper Antivirus to school devices or network	●		●	●	●								
Use of personal digital cameras for capturing images of students/staff and storing images without permission	●	●		●		●	●	●		●			
Accessing and trying to change any other person's username, password, files or data	●		●	●		●		●		●			
Revealing or publicizing confidential school credentials to third person	●		●	●	●	●		●					

SANCTIONS FOR STAFF ON UNACCEPTABLE USE

	Low severity					Medium Severity				High Severity			
Incident Details	Reporting to Immediate Head/Coordinator	Reporting to School Counsellor	Reporting to Online Safety Coordinator/IT coordinator	Reporting to Online Safety Leader/Vice Principal	First Action Plan - Verbal Warning or memo	Reporting to HR	Reporting to Principal/Chairperson	Second Level Plan- written warning letter by the principal	Suspension from job for 2 days	If repeating, Suspension from job more until further notice	Joint decision by School Leadership, Online Safety group and parents	Immediate termination from job and HR submitting a copy of all memos and letters to the concerned authority	Reporting to External Agency/Police
Trying to remove school provided technology resources	●		●	●	●	●		●					
Visiting internet sites that are offensive and trying to post or communicate with staff or schoolmates	●	●	●	●	●	●	●			●			
Indulging in Cyberbullying activities	●	●	●	●		●	●				●	●	●
Promoting any kind of discrimination or racism in online groups	●	●	●	●		●	●				●	●	●

Appendix 1

Acceptable User Agreement for Staff

Eminence Private School recognizes the value of Internet and other digital platform to improve the student learning and enhance the administration and operation of the school. This agreement complies the relevant points from the school's **Acceptable Use Policy (AUP)**.

By signing this agreement, the employee agrees to the terms and conditions listed below.

- Use the school's resources and technologies only for school related purposes.
- Use only school assigned email accounts for online communication.
- Keep passwords and personal information secure and not share with third parties.
- Observe all school Internet filters and posted network security practices.
- Respect the rights, beliefs and viewpoints of others.
- Follow the same standards of behavior online as would be expected to follow in real life
- Report security risks or violations to an authorized personal or IT In-charge.
- Disclose to an authorized personal or the IT In-charge any messages that users receive that are inappropriate or disturbing.
- Protect data, networks, or other digital resources of the school.
- Follow copyright laws.
- Cite sources when using others' work.
- Communicate only in ways that are kind and respectful.
- Ensure that any social networking sites /blogs that are created or actively been contributed are not confused with professional role.
- Ensure that all the data, documents saved, accessed and deleted are in conformance with EPS network protocols.
- Be aware of the fact that unauthorized individuals are not allowed to access ones' school email or other software/technologies provided by Eminence Private School.
- Avoid visiting internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:
    - Pornographic, obscene, vulgar and/or indecent materials
    - Promotion of any kind of discrimination
    - Promotion of racial or religious hatred
    - Promotion of political views
    - Cyber bullying
    - Any other information which may be offensive to colleagues or breaches the integrity of the school or brings the school into disrepute.
- Avoid unauthorized video broadcasting or sharing of files.
- Refrain from using school systems to run a private business.

- Avoid saving inappropriate files to any part of the school issued system, including but not limited to:
    - Music files
    - Movies
    - Video games of all types
    - Offensive images, videos or files
    - Programs which can be used for malicious purposes
- Refrain from using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Eminence Private School.
- Avoid uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Avoid "hacking" and other illegal activities in attempt to gain unauthorized access to restricted files, other devices or computer systems.
- Avoid revealing or publicizing confidential or proprietary information (like financial / personal information, databases, computer / network access codes and passwords)
- Avoid creating or propagating computer viruses or other harmful files.
- Refrain from removing or relocating school-owned technology resources requires prior authorization from the IT Coordinator.
- Carrying out sustained or instantaneous high-volume network traffic (downloading / uploading heavy files) that causes network congestion and hinders others in their use of the internet
- Avoid using the school network for
    - Online gaming and/or gambling
    - Online shopping or any kind of e-commerce
    - Streaming movies of music online
- Refrain from spamming, sending out chain letters, or other mass unsolicited mailings.
- Avoid using personal social media accounts or sites.
- Refrain from using of personal digital cameras or camera phones for taking and transferring images of students or staff without permission and storing images at home without permission.
- Ensure that other person's username, password, files or data shall not be accessed or changed.
- Refrain from connecting any computer or devices including a USB flash drive to the network/ Internet that does not have up to date antivirus software or school recommended firewall system.
- Understand that the failure to comply with this agreement could lead to disciplinary action.

ACKNOWLEDGEMENT

I understand that it is my responsibility to understand and uphold all the terms in the agreement. I also ensure that I shall participate in all training provided.

Employee Name: ________________________________ **Date:** ____________

Job Title: ______________________________

Signature: ________________________________

Note: Any alteration or change of content to this document will be considered null and void.

Acceptable User Agreement for Students

Eminence Private School recognizes the value of the internet and other digital platforms to improve the student learning. This agreement is entered into between the student and Eminence Private School and is in line with the **Acceptable Use Policy** of the school which emphasizes the importance of safe and responsible use of school provided internet and digital platforms. The school reserves the right to vary the terms of this Agreement to accommodate unforeseen circumstances relating to the use of facilities by students.

The following are the terms and conditions the student of Eminence Private School has to comply with while using the school's digital infrastructure and resources:

- Student should use the school provided digital technology and systems for educational purposes only.
- Student should not reveal his/her password(s) to anyone.
- Student should not allow unauthorized individuals to access email/Internet/Intranet/network or other EPS systems.
- Student should ensure that all the documents, and data are saved, accessed and deleted as per the instruction by class facilitator.
- Student should follow online copyright laws.
- Student should use the approved school email and/or other EPS communication systems when communicating with teachers or the school help desk.
- Students should always communicate in ways that are kind and respectful while using the school's email and other school provided communication channels.
- Student must refrain from spamming, sending out chain letters, or other mass unsolicited mailings from the school provided email account.
- Student should not browse, download or send material that could be considered offensive by peers or adults.
- Student should report of any accidental access to, or receipt of inappropriate materials, or filtering breach to class teacher or IT coordinator.
- Student shall not download any unauthorized software, using the school's internet.
- Students shall not indulge in any online activity (while at school) that include but is not limited to:
    - Visit gaming sites
    - Visit e-commerce sites
    - Do business online
    - Visit movies or music streaming sites
    - Visit social media sites
- Student should not use personal digital cameras or camera phones for taking and transferring images of classmates or schoolmates.
- Student should ensure that any social networking sites/blogs etc. that they create or actively contribute to are not confused with their student role.
- Student must understand the dangers of cyber bullying and should be aware about how to report cyberbullying incidents (as informed in workshops by the school).
- Student should avoid unauthorized video broadcasting or sharing of file.

- Student should avoid activities that can that causes network congestion (such as downloading / uploading heavy files) and hinders others in their use of the internet
- Students should not try to access or try to change any other person’s username, password, files or data.
- Student must respect the rights, beliefs and viewpoint of others.
- Student should understand that the failure to comply with this agreement could lead to disciplinary action.

ACKNOWLEDGEMENT

By signing this agreement as a parent, I understand the conditions under which Eminence Private School facilities are made available to my ward. I further understand that additional training and sessions have been provided to my ward on online safety. I understand that my ward may be accessing the school’s internet for educational purposes. I also understand that any use of facilities contrary to this Agreement, or generally, will be treated as a breach of school discipline by my ward and shall be dealt with accordingly.

I, Parent of ____ from Grade ____________ have read, understood, and shall ensure that my child will abide by the above Acceptable Use Guidelines when using Eminence School Educational platforms like ERP, SkoolBeep and Zoom.

Parent Name: _____________________________

Signature: ____________________________ **Date:** ______________________

Note: Any alteration or change of content to this document will be considered null and void.