USE OF TECHNOLOGY

AND

E-SAFETY POLICY

2026-2027

Policy Information			
Created Date	21-06-2026	Reviewed By	Principal
Review Cycle	One Year	Next Review	August 2028
Principal	Dr. Sharmeen Safwan		
Vice Principal	Dr. Yasser		
The author of the policy's role	Department of IT		
Author of the policy	Fasiha Khan	Signature	
Chair of Governors	Ms. Gulnaz Reeha		

Table of Contents

Section	Contents	Page
1	Purpose	3
2	Scope	3
3	What is E-Safety?	3,4
4	The 19 Prohibited Violations (SPEA 2024)	4,5
5	Acceptable & Unacceptable Use — Students	5,6
6	Acceptable & Unacceptable Use — Teaching & Administrative Staff	6,7
7	Acceptable & Unacceptable Use — Parents and Guardians	7,8
8	Roles and Responsibilities	8,9
9	Technical Infrastructure and Security	10
10	Bring Your Own Device (BYOD)	10
11	Digital and Video Images	10,11
12	Reporting and Responding to Incidents	11
13	E-Safety Education	12
14	Data Protection	12
15	Social Media and Professional Identity	13
16	Policy Review and Monitoring	13
Appendix A	Student Acceptable Use Agreement	14

1. Purpose

Happy Home English School is committed to providing a safe, secure and enriching digital learning environment for all members of its community. This policy has been developed to guide the responsible and ethical use of information and communication technology (ICT) across the school, in full compliance with the Sharjah Private Education Authority (SPEA) regulations and the UAE government guidelines on ICT use in educational institutions issued in September 2024 (covering 2025-2028).

The primary objectives of this policy are to:

- Safeguard students, staff, and parents from online risks and harmful content.
- Set clear expectations for acceptable and unacceptable use of technology.
- Promote responsible digital citizenship and ethical online behaviour.
- Ensure compliance with UAE federal laws, SPEA directives, and Ministry of Education (MOE) guidance.
- Empower the school community with the knowledge and skills to use digital tools safely and effectively.

2. Scope

This policy applies to all students, teaching and administrative staff, parents/guardians, volunteers, visitors, and community users who access digital technologies, devices, networks, or online platforms — whether owned by the school or personally owned — within the school premises, during school activities, or on school-provided systems accessed remotely.

This policy should be read in conjunction with:

- HHES Behaviour and Discipline Policy
- HHES Child Protection and Safeguarding Policy
- HHES Anti-Bullying Policy
- MOE Distance eLearning Behaviour Policy
- SPEA Guidelines on IT Use in Private Schools, 2024 (covering 2025-2028).
- UAE Cybercrime Law (Federal Law No. 5 of 2012 and amendments)

3. What is E-Safety?

E-safety refers to the safe and responsible use of digital technology, including the internet and all electronic means of communication — such as email, text messaging, social media, gaming platforms, and web-based applications. In practice, e-safety is as much about behaviour and attitudes as it is about technical safeguards.

Key online risks facing students and staff include:

Content Risks

- Access to illegal, inappropriate, or harmful material online

- Exposure to pornographic, hate-promoting, or extremist websites
- Misinformation and inaccurate content

Contact Risks

- Inappropriate contact with strangers or online predators
- Grooming behaviour and exploitation

Conduct Risks

- Cyberbullying, harassment, and threatening communications
- Identity theft and impersonation
- Sharing personal information or images without permission
- Piracy, plagiarism, and copyright violations

4. The 19 Prohibited Violations (SPEA 2024)

In accordance with SPEA guidelines issued September 2024, the following 19 violations are strictly prohibited for all users of school computers and internet services. Breaches may result in disciplinary action up to and including permanent exclusion from school and referral to relevant authorities.

1	Using email or any digital platform to threaten, harass, or intimidate others.
2	Sending, posting, or distributing disturbing, offensive, or harmful images online.
3	Using the internet for any form of piracy — including unauthorised downloading of music, movies, games, or software.
4	Sharing, using, or disclosing another person's password or login credentials.
5	Violating copyright laws by downloading, copying, or distributing electronic files for personal use without proper authorisation.
6	Sharing confidential school matters or information with unauthorised individuals or parties outside the school.
7	Compromising the school's electronic systems by introducing malware, viruses, or other malicious software.
8	Using school internet or devices for personal purposes unrelated to education.
9	Visiting or accessing websites that are not authorised or blocked by the school's content filtering system.
10	Distributing inaccurate, offensive, defamatory, or misleading information online.
11	Using inappropriate, threatening, or abusive language in any digital communication.
12	Intentionally damaging, tampering with, or misusing school devices or software.

13	Deliberately causing harm to another person's digital work, files, or programs.
14	Engaging in any form of cyberbullying, including online harassment, intimidation, or targeted abuse.
15	Impersonating another person online or using someone else's digital identity.
16	Plagiarising others' work or misrepresenting AI-generated content as one's own.
17	Accessing pornographic, hate-promoting, extremist, or otherwise inappropriate websites.
18	Disclosing personal information (of self or others) online without explicit permission.
19	Accessing social media sites without express teacher permission and/or for non-educational purposes.

5. Acceptable & Unacceptable Use — Students

5.1 Acceptable Use of Technology for Students

Students are permitted to use school-provided technology and internet access for the following purposes:

- Using web browsers for educational research and gathering information from approved websites and databases.
- Using the internet to share documents and collaborate on tasks that promote teamwork and group learning.
- Participating in online assessments, tests, or tasks approved or recommended by teachers.
- Studying curriculum content online and completing related tasks as assigned by teachers.
- Working on school projects, lesson presentations, and subject assignments.
- Accessing exam preparation sites and official practice papers.
- Preparing digital materials for school community events (circulars, invitations, booklets) with prior teacher approval.
- Accessing social media sites for educational purposes only, under direct teacher supervision and guidance.
- Communicating via school-approved platforms using appropriate, respectful language at all times.
- Taking care of all digital devices provided or used at school.
- Students may bring one approved personal learning device (Chromebook).
- Maintaining confidentiality of personal usernames, passwords, and login credentials at all times.

5.2 Unacceptable Use of Technology for Students

The following actions are strictly prohibited and will result in disciplinary action in line with the school's Behaviour Policy and SPEA regulations:

- Bringing mobile phones, smart watches, or personal cameras to school (monitored by surveillance cameras). The school accepts no liability for personal devices brought to school without authorisation.
- Using the internet to send, download, or publish offensive, immoral, or illegal material that violates UAE laws, SPEA regulations, or Islamic values.
- Photographing, recording, or videoing teachers, students, or school staff and posting such content on any media without prior written permission.
- Impersonating another person or accessing another student's personal accounts or data.
- Downloading any program, application, game, video, or file that is not for educational purposes or has not been authorised by the relevant teacher.
- Engaging in any form of cyberbullying, harassment, or discrimination — whether on school premises or off-campus if related to the school community.
- Publishing content that incites hatred, racism, sectarianism, or that disturbs public order or Islamic values.
- Promoting any commercial product, service, or conducting fundraising without authorisation.
- Downloading or distributing commercial software or any material protected by copyright and intellectual property rights without a valid licence.
- Attempting to bypass the school's internet filtering systems through VPNs or proxy tools (restricted under UAE law).
- Using AI tools to cheat, plagiarise, or misrepresent artificially generated work as one's own.
- Attempting to access, modify, or delete another user's files, accounts, or data.
- Sharing passwords or login credentials with any other person.
- Initiating or engaging in online communication with members of the opposite gender in violation of SPEA guidelines and school values.

6. Acceptable & Unacceptable Use — Teaching & Administrative Staff

6.1 Acceptable Use for Staff

- Using the internet exclusively for school-related educational, administrative, or professional development purposes.
- Using school-issued email for work-related correspondence only.
- Participating in professional development activities, online research, and approved training programmes.

- Using all available online educational resources, platforms, and tools to support teaching and learning.
- Employing technology in innovative ways to stimulate student engagement and develop 21st Century skills.
- Checking and verifying the accuracy of digital content before sharing with students.
- Citing and crediting the source of any digital content used in teaching materials.
- Downloading and installing programs on school devices only after approval from the Digital Safety Officer (IT Coordinator).
- Publishing photos or videos of students on school-related platforms only with explicit consent from the school administration and parents.
- Raising student awareness of their rights, responsibilities, and safe use of digital technology.
- Reporting any technological security concerns, policy violations, or suspected misuse to the school's IT Coordinator or Discipline Committee promptly.
- Changing passwords periodically and maintaining the confidentiality of login credentials.

6.2 Unacceptable Use for Staff

- Using school devices or networks for personal purposes unrelated to school functions.
- Sharing work usernames and passwords with other employees or students.
- Sending, uploading, or publishing material that incites hatred, racism, or sectarianism, or that harms national unity.
- Sharing confidential information about the school, students, or staff with unauthorised parties.
- Downloading or showing students content that contradicts school policies or Islamic values.
- Failing to attribute the source of digital content or copying copyrighted materials without proper licensing.
- Hacking, disrupting the network, or attempting to gain unauthorised access to systems or accounts.
- Using personal social media to reference students, parents, or colleagues, or to post content that could harm the school's reputation.
- Publishing photos or videos of students without prior approval from the school administration.
- Saving personal data or using personal accounts on school devices.
- Using school email for personal correspondence.

7. Acceptable & Unacceptable Use — Parents and Guardians

7.1 Acceptable Use for Parents

- Accessing the internet via the school's guest Wi-Fi network for lawful, school-related purposes only.
- Communicating with the school through official channels using respectful, appropriate language in accordance with UAE laws.
- Copying or sharing school-related photos or videos only after receiving explicit written approval from the school administration.
- Reporting any security concerns or suspected misuse of the school's digital platforms to the IT Coordinator or Discipline Committee immediately.
- Instructing children to maintain the confidentiality of passwords and login credentials for all school systems.
- Actively supporting the school in promoting good e-safety practices at home.

7.2 Unacceptable Use for Parents

- Using the school's Wi-Fi network to access inappropriate, offensive, or illegal content.
- Photographing or recording students, staff, or school activities without prior written permission from the administration.
- Using social media to post offensive, defamatory, or inappropriate comments about the school, its staff, or the wider school community.
- Accessing or attempting to access unauthorised systems, or downloading software that could introduce malware to school devices.
- Sharing, distributing, or posting images or videos of students other than their own children on social media or public platforms.
- Engaging in any form of cyberbullying targeting students, staff, or other parents — the school will take legal action in accordance with UAE cybercrime laws.
- Downloading commercial software or copyright-protected materials without a valid licence.
- Withholding information about identified security incidents or misuse of school platforms.

8. Roles and Responsibilities

a) Board of Governors / School Management

- Approve and periodically review this E-Safety Policy.
- Receive regular reports on e-safety incidents, monitoring outcomes, and policy effectiveness.
- Ensure that an E-Safety Governor role is designated, with responsibility for monitoring incident logs and meeting with the E-Safety Coordinator.

b) School Principal and Senior Leadership Team (SLT)

- Maintain overall duty of care for the safety of all members of the school community, including e-safety.
- Ensure the E-Safety Coordinator and all relevant staff receive appropriate and up-to-date training.
- Establish systems for monitoring and supporting staff who carry out internal e-safety monitoring roles.
- Be aware of the procedures to be followed in the event of a serious e-safety allegation against a staff member.

c) E-Safety Coordinator (Digital Safety Officer)

- Lead day-to-day responsibility for all e-safety matters and policy development.
- Ensure all staff are aware of incident reporting procedures.
- Provide training, guidance, and advice for staff, students, and parents.
- Maintain and review the log of e-safety incidents.
- Liaise with SPEA, IT technical staff, and the Child Protection / Safeguarding Lead.
- Report regularly to SLT and meet with the E-Safety Governor.

d) IT Coordinator and Technical Staff

- Ensure the school's technical infrastructure is secure and protected from misuse or malicious attack.
- Implement and maintain content filtering, firewall, and monitoring systems in line with SPEA requirements.
- Ensure all users access the network via enforced password protection, with regular password changes.
- Regularly monitor and record user activity on school systems, reporting any misuse to the E-Safety Coordinator or Principal.
- Keep up to date with emerging e-safety technical guidance and apply relevant updates.

e) Teaching and Support Staff

- Maintain an up-to-date awareness of e-safety matters, this policy, and current best practices.
- Read, understand, and sign the Staff Acceptable Use Agreement.
- Report any suspected misuse, incidents, or concerns to the Head of Year or E-Safety Coordinator promptly.
- Ensure all digital communications with students and parents are conducted professionally and only via official school channels.
- Monitor students' use of digital technologies in lessons and implement current policies on devices.
- Guide students to pre-approved, age-appropriate websites in pre-planned internet lessons.

- Embed e-safety messages across the curriculum and pastoral activities.

f) Child Protection / Designated Safeguarding Lead (DSL)

- Be trained in e-safety issues and aware of the potential for serious child protection concerns arising from online activity.
- Identify and respond to risks including: sharing of personal data, access to illegal material, inappropriate adult contact, grooming, and cyberbullying.
- Maintain accurate and confidential records of all safeguarding incidents and follow-up actions.
- Report allegations or suspicions to the Principal and, where required, to SPEA or UAE authorities.

g) Students

- Use school digital technology systems in accordance with this policy and the Student Acceptable Use Agreement.
- Report any abuse, misuse, or access to inappropriate materials to a trusted adult or teacher immediately.
- Understand and respect policies on mobile devices, digital cameras, and the taking and sharing of images.
- Adopt good e-safety practices both within and outside school, recognising that this policy extends to actions that affect the school community regardless of location.

h) Parents and Guardians

- Support the school in reinforcing good e-safety habits at home.
- Attend school awareness sessions, consult school newsletters and the school website for e-safety guidance.
- Follow school guidelines on appropriate use of digital images taken at school events.
- Ensure children understand acceptable use expectations for personal devices.

9. Technical Infrastructure and Security

Happy Home English School will ensure that its technical infrastructure supports a safe and secure digital environment:

- All school internet access is filtered and monitored for all users, with filtering calibrated appropriately to user age and role.
- Servers, wireless access points, and cabling are physically secured with restricted access.
- All users are assigned clearly defined access rights with unique login credentials.
- Virus protection and security software on all school devices is kept fully up to date.
- A guest network (Wi-Fi) is provided for parents and authorised visitors, with access restricted to appropriate use.

- Personal data cannot be transmitted over the internet or removed from school premises unless securely encrypted.
- Regular audits of network security, software licences, and system integrity are conducted and logged.
- An agreed procedure exists for granting temporary access to guest users (e.g., supply teachers, visitors) with appropriate safeguards.
- The school reserves the right to inspect any device — including personal devices — used on its premises where reasonable cause for concern exists.

10. Bring Your Own Device (BYOD)

Where the school permits students to bring personal devices for learning, the following conditions apply:

- Only one approved personal device (Chromebook) may be brought.
- Mobile phones are NOT permitted on school premises. Violations will be monitored via surveillance cameras.
- Personal devices must be clearly labelled, secured with a password or biometric lock, and kept in good condition.
- Students are solely responsible for the security and care of their personal device. The school accepts no liability for loss or damage.
- Personal devices must be connected to the school network only and filtered under the school's normal internet safeguards.
- Devices may not be shared with other students.
- Any VPN, proxy, or circumvention tool is strictly prohibited (restricted under UAE law).
- Any breach of BYOD conditions may result in confiscation of the device and further disciplinary action.

11. Digital and Video Images

- Staff may only take digital or video images of students for legitimate educational purposes, in line with school policy.
- Parents may take digital images or videos of their own children at school events for personal use; these must not be posted publicly on social media or shared without permission.
- Images or videos of students must not include other identifiable children without their parents' written consent.
- Students' full names must never appear alongside photographs on the school website, social media, or any other public platform.
- Written parental consent must be obtained before any student photographs are published on the school website or official channels.

- Students must not record, photograph, or distribute images of others without explicit permission — violations are an offence under UAE law.

12. Reporting and Responding to Incidents

All members of the school community are expected to report e-safety concerns promptly. The following procedures apply:

Reporting Channels

- Speak directly to a trusted teacher, Head of Year, or the E-Safety Coordinator.
- Submit via the school's anonymous complaint box at the reception.
- Contact the school office or email the designated safeguarding address.

Response Procedures

- Any suspected illegal activity — including child sexual abuse imagery or grooming — will be reported immediately to the UAE authorities / police.
- All investigations will be conducted by at least two senior staff members to safeguard all parties.
- The device(s) involved will be preserved, and the URL/content documented; screenshots may be taken where appropriate.
- Completed incident reports will be retained as evidence and may be referred to the relevant authorities.
- Disciplinary action will be taken in accordance with the school's Behaviour Policy and SPEA regulations.
- The school will notify parents/guardians of relevant incidents involving their children.

Consequences for Policy Violations

- Removal of access to school network, internet, and digital systems.
- Confiscation of personal device.
- Parental notification and meeting.
- Disciplinary measures in accordance with the school's Behaviour Policy (Sanctions Ladder).
- Referral to SPEA or UAE law enforcement for illegal activity.
- Fixed-term or permanent exclusion from school for serious or repeated violations.

13. E-Safety Education

E-safety education is embedded across the curriculum and reinforced through pastoral programmes, assemblies, and whole-school initiatives. Key areas of e-safety teaching by stage:

Key Stage 1 (FS2)

- Using technology safely and respectfully.
- Keeping personal information private.
- Identifying where to seek help and support.

Key Stage 2 (Year 1 – Year 6)

- Never sharing personal details (address, phone number, photos, school name) with online contacts.
- Understanding the risks of sharing images online and why meeting online friends in person is unsafe.
- Recognising spam and phishing; not responding to unsolicited messages.
- Understanding that online identities may be falsified.
- Recognising and reporting cyberbullying.

Key Stage 3 (Year 7)

- Reinforcing all prior e-safety knowledge with greater depth and complexity.
- Staying safe on social networking platforms: privacy settings, age restrictions.
- Understanding digital footprints and their long-term consequences.
- Digital citizenship, ethical online conduct, and intellectual property.
- Dangers of VPN misuse, bypassing school filters, and UAE cyber law implications.
- Responsible use of AI tools and the importance of academic integrity.

The school will also engage parents through newsletters, school website updates, Parents' Evenings, coffee mornings/webinars, and participation in national campaigns such as Safer Internet Day.

14. Data Protection

Happy Home English School processes personal data in accordance with applicable UAE data protection legislation. Personal data will be:

- Collected and processed fairly, lawfully, and for clearly defined educational purposes only.
- Adequate, relevant, accurate, and not held for longer than necessary.
- Kept secure and protected against unauthorised access, loss, or misuse.
- Only transferred to third parties with adequate safeguards in place.

Staff must ensure that personal data is accessed only on secure, password-protected devices, and that sessions are properly logged off. Data may not be transferred externally without secure encryption.

15. Social Media and Professional Identity

Staff are reminded that their use of personal social media may reflect on the school and must adhere to the following:

- No reference should be made on personal social media to students, parents, or colleagues.
- Personal opinions must not be attributed to the school or SPEA.
- Security settings on personal social media profiles should be regularly reviewed.
- Staff must not engage in online discussions on personal matters relating to members of the school community.

Violations may constitute misconduct and could result in disciplinary action, or civil and criminal liability under UAE law.

16. Policy Review and Monitoring

This policy will be reviewed annually (or sooner if required by changes in technology, SPEA guidance, or UAE legislation). The E-Safety Coordinator will monitor the impact of this policy through:

- Logs of reported e-safety incidents.
- Regular audit reports from the IT Coordinator.
- Lesson observations and curriculum monitoring.
- Student, staff, and parent surveys.
- Meetings with students, staff, parents, and governors.
- Participation in national e-safety awareness events (e.g., Safer Internet Day).

APPENDIX A

Student Acceptable Use Agreement

Happy Home English School — Academic Year 2026-2027

I, the undersigned student, confirm that I have read, understood, and agree to comply with the Happy Home English School Use of Technology and E-Safety Policy. I understand that:

- I will use school digital systems responsibly to keep myself, other students, and the network safe.
- Access to the school network and internet is a privilege, not a right, and may be withdrawn if I violate this agreement.
- I am responsible for my actions when using digital devices, both on and off campus, where these affect the school community.
- I will only bring one approved personal learning device (Chromebook) to school when required.
- Mobile phones are NOT permitted on school premises.
- I will keep all login credentials private and will never share passwords with anyone.
- I will use the internet and digital resources only for approved school educational purposes.
- I will not attempt to install software, use VPNs, or bypass the school's internet filters.
- I will communicate respectfully and use appropriate language in all digital interactions.
- I will not engage in cyberbullying, harassment, or any behaviour that may harm others.
- I will not record, photograph, or distribute images of others without explicit permission.
- I will immediately report any inappropriate, harmful, or offensive content to a teacher or trusted adult.
- I understand that the school may inspect my personal device if there is reasonable concern about misuse.
- Violations may result in loss of device access, disciplinary action, and referral to authorities where UAE law has been breached.

Student	**Parent / Guardian**
Full Name: _____	Full Name: _____
Class / Year: _____	Relationship: _____
Signature: _____	Signature: _____
Date: _____	Date: _____

The school reserves the right to take the measures it deems appropriate in accordance with SPEA regulations and UAE law against those who violate this policy.