Digital Safeguarding Policy

School Vision, Mission and Core Values

Our Vision

Providing world-class education

Our Mission

To empower students with a holistic, rigorous and international education for success in an ever-changing world

Core Values

Achievement | Collaboration | Innovation | Integrity | Respect | Responsibility

Adopted: August 2023
Reviewed: July 2025
Next review: July 2026

CEO/Board	**Principal**

Head of Primary School	**Head of Secondary School**	**Safeguarding Governor**

Summary of Contents:

1.	Introduction	3
2.	Aims	3
3.	Rationale	3
4.	Guidelines	4
5.	Mobile device monitoring	4
6.	Netiquette	4
7.	Collaboration and storage system	5
8.	Cyberbullying	5
9.	Key roles and responsibilities	6
10.	E-safety	10
11.	Reporting process	13
12.	Bring Your Own Device (BYOD)	13
13.	Device Guidelines	13
14.	Device Violations	14
15.	Use of AI	14
16.	Other Related Policies	15
17.	Additional resources	15
18.	Policy monitoring and review	15
19.	BYOD Acceptable Use Agreement	16

Introduction:

Raffles International School recognises that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for their exciting futures. We are committed to helping students develop digital literacy and communication skills and provide infrastructure access to technologies for student use.

Aims:
At Raffles International School, we aim to ensure that staff, students, and parents are committed to safe and effective digital literacy practices, using the internet and other digital technologies to:

- Increase student opportunities to develop skills in the digital world
- Prepare students for using technology safely both inside and outside of school
- Make learning exciting and interactive
- Increase variation within lessons, broadening learning experiences
- Raise educational standards
- Provide students with opportunities to access a wide variety of knowledge in a safe way

This policy aims to ensure that technology and online use at Raffles International School is appropriate, responsible, and in line with UAE laws.

Rationale:
Wellbeing and achievement are central to Raffles International School, allowing us to grow as lifelong learners and take responsibility for ourselves and the community. Students can expect a 21st century learning environment at RIS where teachers work to integrate technology thoughtfully and purposefully in learning experiences and assignments. Students can also expect access to appropriate devices and network services that support the curriculum of the school.

This Digital Safeguarding Policy is specifically tailored for Raffles International School. It addresses all aspects of online and offline activities and behaviour, including the use of both school-owned and personal devices by students and staff. The primary goal of this policy is to safeguard students and staff and ensure they maintain digital safety practices within and beyond the school environment. This policy is designed to reduce risks to students. Additionally, the policy is designed to protect employees and the school whilst upholding professional standards.

Guidelines
The importance of digital safeguarding is evolving rapidly alongside technological advancements. Raffles International School recognises the necessity of actively and promptly managing risks to ensure effective digital safeguarding. Many issues that occur in digital safeguarding are behavioural, and managing incidents often run parallel to the efforts to promote appropriate conduct in other aspects of school life or professional activities.

In order to use the school's digital resources, students and staff must follow the guidelines set forth in this policy. The rules written in this agreement are not all inclusive. RIS reserves the right to change this agreement as and when deemed necessary to do so. It is a general agreement that all facilities (hardware, software, internet, etc.) are to be used in a responsible, ethical, and legal manner, in and out of school. By using any digital resources, whether owned personally or by the school, users acknowledge their understanding of the policy as a condition of using such devices and the internet.

The guidelines provided in this policy are intended to help users understand appropriate use. The school may restrict, suspend, or terminate any user's access to the school's computer systems upon violation of this policy. This policy applies to all digital resources, not only the computers, devices and equipment provided in the school's IT labs, but also the personal devices students bring to school in accordance with the school's Bring Your Own Device initiative.

Students and staff should look after and care for their devices. A protective case and screen is recommended. RIS takes no responsibility for the loss or damage of devices. Users are expected to treat equipment with extreme care and caution; these are expensive devices that are entrusted to their care. Staff should report any damage or loss to their school device to the IT department immediately.

Mobile Device Monitoring

The school will use security systems to filter objectionable materials on the internet in order to help ensure the safety of all students. Access to the internet, including web sites, content, and online tools will be restricted in compliance with UAE regulations and RIS policies. Web activity logs are recorded in security systems.

Netiquette

- Users should not attempt to open files or follow links from unknown or untrusted origin.
- Recognising the benefits collaboration brings to education, RIS provides students with access to web sites or tools that allow communication, collaboration, sharing, and messaging amongst students. Students are expected to communicate with appropriate, safe, mindful, courteous conduct online as is expected offline.
- Playing commercial/online games and visiting sites not related to education are not permitted. Watching movies, TV shows, etc. while at school is prohibited.
- Respect the use of copyrighted materials. Respect the rights and privacy of others.
- Installation of software and applications on students' own devices is permitted as long as it does not conflict with the security requirements outlined above or the primary purpose of such devices as learning tools. Downloading of unauthorised programs is not allowed.
- Modifying or copying any protected system files, system folders, or control panel files on school equipment are strictly prohibited.
- Obey the laws and restrictions of UAE, do not use personal equipment to record (audio/visual) others without their permission and upload them.

- Alert a teacher or other staff member if you see threatening, appropriate, or harmful content (images, messages, posts) online and help maintain the integrity of the school network.
- You should use trusted sources when conducting research via the Internet.

Collaboration and storage system

The school provides students with official email accounts via Microsoft Office 365, granting them access to various tools such as OneDrive and Teams. These resources facilitate collaboration and allow students to share and store their work and assignments throughout the academic year, helping them build an electronic portfolio. As per the school's BYOD policy, students are responsible for backing up their own data.

Cyberbullying

Cyberbullying means bullying by electronic means which occurs through the use of technology, including computers or other electronic devices, social networks, text messaging, instant messaging, websites, or e-mail.

Students need to be fully aware of their responsibilities as digital citizens. These responsibilities are reinforced at school via the curriculum. This provides the students with a clear understanding of the above conditions within the UAE, and includes comprehensive coverage of issues relating to students' own 'digital footprints' and creating a positive online presence, as well as interaction with others. Through the curriculum, students will be educated on the dangers of technologies and online communication. They will be guided on the importance of appropriate online behaviours, and how to use technology safely.

Cyberbullying will not be tolerated. Harassing, slandering, denigrating, impersonating, outing, tricking, excluding, and cyber stalking are all examples of cyber bullying. Students should not send emails or post comments with the intent of scaring, hurting, or intimidating someone else. Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in disciplinary action. In some cases, cyber bullying can be a crime. Remember that your activities are monitored and retained.

Students will be held accountable for cyberbullying, even if it occurs off-site during the school year and negatively impacts the academic environment at RIS. Students are reminded that in the UAE there are extreme consequences for online defamation of character of person or organisation.

The Federal Law No. 5 2012, was issued by the President his Highness Sheikh Khalifa Bin Zayed Al Nayhan and is commonly known as the 'Cyber Crimes Law'. It is the Cyber Crimes Law that provides the most practical recourse for victims of crimes involving technology. Article 20 deals with slander: '*any person who insults a third party or has attributed to him an incident that may make him subject to punishment or contempt by a third party by using an Information Network or an Information Technology Tool shall be punished by imprisonment and a fine not less than (AED 250,000) and not exceeding (AED 500,000) or by any of these punishment's.* Article 16 of the Cyber Crimes Law states that a perpetrator of an action that could be considered to be extortion '*shall be punished by imprisonment for a period of two years at most and a fine not less than AED 250,000 and not in excess of AED 500,000, or either*

of these two penalties'. Accordingly, threatening to bully someone unless money is received may lead to severe penalties – the act of bullying does not have to eventuate, it can simply be threatened. If the extortioner uses the threat of bullying (eg; "I'll tell everyone that you...") in order to extract money or something of value from the victim, they may be found guilty under this law. Article 15 of the New Cyber Crimes Law also states that it is an offence for persons to intentionally and without permission capture and/or intercept communications online.

The consequences are both emotional and educational. Cyberbullying differs from other methods of bullying and has several key differences:

- Cyberbullying can happen any time and any place and for many young people home is no longer a safe place from bullying.
- Online communication between young people is often hidden from adults and free from supervision.
- The anonymity the internet offers has consequences such as the targets don't know the identity of their bullies which can lead to the 'victim' refraining from communicating with all others.
- Young people who post online are not as responsible for their actions as they should be, usually through ignorance of the permanence of the post. They are usually not immediately confronted with the consequences of their actions as they might otherwise, which makes them less 'fearful' of being punished.
- Digital content can be shared and seen by a large audience almost instantly and is almost impossible to delete permanently.
- Young people are often fearful of reporting incidents, as they fear the adults will take away their devices.

Safeguarding staff including Heads of Year and the DSL will act to deal with any suspected cyberbullying issue. This might include a conversation with the child, a conversation with the perpetrator, safeguarding conversations, contact with parents, contact with the counsellor etc. The safeguarding and behaviour policies will guide decisions made and actions taken. Each incident will be dealt with on a case by case, consulting the behaviour policy. Both the 'bully' as well as the 'victim' will be offered emotional support and guidance.

Key Roles and Responsibilities

Many senior leaders are trained in safeguarding practices and procedures. The Senior Leadership Team ensures digital safeguarding is given a suitably high priority. All members of staff must be appropriately trained annually (and when a pressing development arises) in digital safeguarding by the Designated Safeguarding Leads.

Designated Safeguarding Lead (DSL)

- Create and update supporting documentation and resources and arrange training around acceptable use of technology at RIS.
- Monitor and review digital safeguarding training and education for staff, parents and students alongside the school's IT department.
- Develop staff, parent and student understanding of digital safeguarding through implementation and use of resources available.

- Take an active role in supporting disclosures made that have a digital safeguarding concern.
- Undertake appropriate training to acquire a detailed insight into current concerns and consequences of particular digital safeguarding situations and actions.
- Be aware of the potential for serious child protection / safeguarding issues to arise from:
    - Sharing of personal data
    - Access to illegal / inappropriate materials
    - Inappropriate on-line contact with adults / strangers
    - Potential or actual incidents of grooming
    - Cyberbullying
- Ensure members of staff are informed about lines of external support that are available.
- Monitor, develop and keep up-to-date the Digital Safeguarding Policy which must accurately reflect the requirements of the Raffles International School community.
- Develop, write and review an acceptable BYOD Acceptable Use Policy and ensure these are signed by children and parents where applicable.
- Ensure that the above documentation is filed for future reference if required.
- Ensure there are clearly understood measures for staff and students to deter and reform inappropriate behaviour.
- Ensure that public communications on behalf of the school through digital channels, including social media, are appropriately managed and consistent with all applicable policies.
- Ensure that our digital safeguarding programme is taking place by monitoring planning and ensuring there are assemblies on E-Safety issues throughout the year in each phase of the school.

Staff members

- Act on all digital safeguarding issues promptly and in accordance with this Digital Safeguarding Policy.
- Be diligent when digital safeguarding issues suggest child protection concern: follow child protection procedures immediately in line with the RIS Safeguarding and Child Protection policy.
- Work within the schools digital safeguarding measures and not attempt to compromise or circumvent those measures.
- Protect professional boundaries by, for example, not giving students a member of staff's mobile number, not allowing a staff network log-in to be used by a student and not becoming 'friends' or 'contacts' with students on social media sites.
- Be diligent in respect of data protection.
- Select websites for school use only after reviewing Terms and Conditions, especially in regard to data protection compliance and minimum permitted age.
- Seek advice from the school's Designated Safeguarding Lead whenever necessary to discuss concerns, develop best practice and support students.
- Not engage in one-to-one online meetings with students.
- Should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:
    - Sharing of personal data

- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyberbullying

Students

- Work within the school's digital safeguarding measures and try not to compromise or bypass these measures.
- Know both whom, and how to report anything that could improve the digital safeguarding environment and the digital/online wellbeing of students.
- Respect personal privacy and keep their own personal information private, including photographs and passwords.
- Password guidance is as follows:
  - Change password from the preset versions.
  - Do not use an obvious secret question e.g. Name of their school.
  - Use a mix of uppercase and lowercase letters, numbers, and special characters e.g.,!@#?. Aim for at least 8 characters to enhance security.
  - Avoid Common Passwords do not use easily guessable passwords such as "password123," your name, or birthdates.
  - Change your passwords periodically to protect against unauthorized access. School recommends students & staff to change password in every 90 days.
  - Keep your passwords confidential and do not share them with anyone, including colleague's friends or classmates.
- Do not share any personal information or photographs of other students and staff or any text and images that contravenes UAE laws, including the UAE Cybercrimes Law. Any publication or sharing of photographs of other individuals without the consent of that individual is a crime under the UAE Cybercrimes Law (Law No. 34 of 2021).
- Never log in to another person's account without their permission. Even if the password is known, this is a criminal offence.
- Behave in a healthy and positive manner towards digital technologies when engaging in online activities.
- When engaging in online activities being aware of the dangers which can arise from:
  - Sharing of personal data
  - Accessing illegal / inappropriate materials
  - Engaging in inappropriate on-line contact with adults / strangers including the potential or actual incidents of grooming
  - Cyberbullying
- Read and respect (or ask for advice and permission as appropriate) the Terms and Conditions of web services, especially with regard to the minimum age that some companies set for their websites in order to protect young people from risk.
- Do not create social media accounts which include the Raffles International School name and/or logo.
- Do not create any social media accounts under a name other than their own with the intention of using the anonymity inappropriately.
- Sign (digital) the BYOD Acceptable Use Policy and understand what the agreements mean.

IT Team

- Security systems that are put in place to reduce and, where possible, prevent inappropriate behaviour and the accessing of unacceptable content.
- Manage and maintain different user profiles for web filtering to provide protection as appropriate and flexibly as required.
- Timely update/reporting web filtering and reporting of any malicious activity/incidents to the safeguarding team/Principal.
- Conduct active testing to ensure that blocked content remains inaccessible.
- Monitor the selection of all web based services by members of staff to ensure use is consistent with the terms and conditions (including minimum age)
- Encourage appropriate use of file storage locations.
- Ensure procedures are in place to prevent digital safeguarding decisions being taken by technical staff.
- Convey clear messages and employ workable measures to discourage users from connection to external networks whilst on school premises.
- Monitor the school online profile and presence, on public platforms.
- The school has a skilled IT team available to assist with technical-related issues.

Parents

- Discuss the school's BYOD Acceptable Use Policy with their child(ren) and explain its implications at school and at home.
- Access support systems in school and via the internet to develop appropriate awareness of how to protect their child.
- Talk through concerns about digital safeguarding with an appropriate member of staff as necessary.
- Know whom and how to report concerns in order to improve the digital safeguarding environment and protect their child both at home and at school.
- Work with the digital safeguarding measures the school has in place.
- Respect digital safeguarding and data protection advice when sharing images, videos and text, especially personal information on social networking sites.
- Respect school passwords and encourage their child never to attempt to obtain or use another child or adult's password.
- Refrain from posting anything online or on social media which can be seen to be defaming the school in any way.
- Whilst on the school site refrain from taking photos/videos, including during sporting matches and drama performances of any child other than their own. Under no circumstances should parents be sharing images of other children, or information that identifies other children, on social media. Note also that the publication or sharing of images or videos of other individuals without their consent is a crime under the UAE Cybercrimes Law.
- Encourage their child to read and respect (or ask for advice and permission as appropriate) the Terms and Conditions of web services, especially with regard to the minimum age that some companies set for their websites in order to protect young people from risk.

E-safety

E-safety refers to keeping users safe while using electronic devices and accessing material, such as the internet. Our school is committed to ensuring the e-safety of all its members. We will achieve this through education, technology, accountability, and responsibility. Within our school, both staff and students share the responsibility for e-safety, with specific duties assigned to each group.

Teaching Staff E-safety Responsibilities

- All digital communications with students/parents/carers should be on a professional level and only carried out using official school systems, such as ISAMS, Class Charts and Class Dojo.
- Staff should **never** share their personal mobile number, nor be communicating with parents through Whatsapp or other messaging services.
- Have up-to-date awareness of e-safety matters.
- Report any suspected misuse or problems the students encounter to the Heads of Year and/or the IT Team.
- Lock their laptop/desktop screen if they leave their device, even if it is for a short time. Staff should log out of their RIS account at the end of every day.
- Ensure E-safety issues are embedded in all aspects of the curriculum and other activities. Monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed), and implement current policies with regard to these devices In lessons. Where internet use is pre-planned, students should be guided to sites that have been pre-checked for suitability.
- Respect personal privacy and keep their own personal information private, including photographs and passwords.
- Do not share any personal data or photographs of students or staff or any text and images that contravenes the Laws, including the UAE Cybercrimes Law and the UAE Copyright Law (Law No. 38 of 2021), notably: *The "use of information network, electronic information system or information technology methods, for the purpose of breaching the privacy of a person or private or family life of individuals without consent, other than legally permitted, shall be sentenced to detention for a period of not less than (6) six months and/or to pay a fine of not less than (150,000) one hundred fifty thousand Dirhams and not more than (500,000) five hundred thousand Dirhams". This includes "Taking photographs of others at any public or private place or preparing, communicating, exposing, copying or keeping electronic images thereof".* Article 44 of the UAE Cyber Crime Law. *It is not "permissible for anyone with whom it has been agreed to take a photograph of another or sound or visual recording, in any way whatsoever, to keep, publish, exhibit, or distribute the original or Reproductions thereof without the permission of that person, unless otherwise agreed upon".* Article 45 of the UAE Copyright Law.
- Behave in a healthy and positive manner towards digital technologies when engaging in online activities.
- Read and respect (or ask for advice and permission as appropriate) the Terms and Conditions of Web Services (for example - Google Terms and Conditions)
- In relation to staff members personal social media accounts: Posts should be positive and professional. Confidential, proprietary or privileged information about other staff,

students, parents/carers, or school projects, policies or finances should never be posted or published.

- Do not interact with students or parents on social media platforms.
- Accounts should be set to private and deny friend or message requests from students.
- Staff in doubt about professional social media use should ask for guidance from a member of SLT or Safeguarding Le.
- Be aware of how to spot incidents of cyberbullying within the school environment.
- Staff who have been informed of any inappropriate online behaviours are to add to ISAMS (Primary) or Class Charts (Secondary) if this is a behaviour related issue. If there are any safeguarding concerns, then it should **also** be recorded following the school's safeguarding reporting procedures.

Students E-Safety Responsibilities

- Behave responsibly and appropriately when using communication technology, including the internet and online platforms.
- Students should not use messaging services (ie Whatsapp, iMessage) on devices that are used for learning during the school day.
- Do not walk around school site using devices (e.g. in the corridors between lessons) as this could cause potential harm or damage to devices.
- Lock their screen if they leave their device, even just for a short period of time.
- Use the school BYOD wifi network for gaining access to the internet; no access should be provided by the use of data plans.
- Copyright/intellectual property rights and UAE laws must be respected.
- E-mail and posts on Microsoft Teams should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers.
- Should not share personal information, including phone number, address, ID number, passwords, school email password, any e-resources issued by school, or birthday over the internet, without adult permission.
- Should recognise that communicating over the internet brings anonymity and associated risks so should carefully safeguard the personal information of themselves and others.
- Should not agree to meet someone they met online in real life without parental permission.
- If they see a message, comment, image, or anything else online that makes you concerned for their personal safety, bring it to the attention of an adult (teacher if they are at school; parent if they are using the device at home) immediately.
- Should recognise that some valuable content online is unverified, incorrect, or inappropriate in content.
- Should not post anything online that they would not want parents, teachers, future schools, employers or the UAE government to see.
- Be responsible for email they send and for contacts made. Anonymous messages, chain letters, are not permitted. "Spamming", cyber bullying and the use of chat rooms is not permitted.
- Access to sites containing illegal, offensive, pornographic, racially or religiously offensive material is not allowed and may be a crime under the UAE Cybercrimes Law

- Compromising or damaging the security or stability of the network is not allowed
- Only use approved email accounts on the school system for school purposes.
- Immediately inform a teacher or trusted adult if they receive an offensive or inappropriate email or communication from an unknown source.
- Be aware of the steps of grooming and be aware that people online are not always who they say they are.
- Be responsible for all activities that are carried out under their school email/personal email. RIS will not be liable where their password or user name is used by someone else.
- Inform their form tutor or Head of Year of any unauthorised use of their password or user name of which they become aware. RIS IT team have the right to disable any user account or password at any time if we confirm any breach of the policy.
- When signing in to a public device with their school email and password make sure to log out afterwards.
- Do not share any personal data or photographs of other students or staff or any text and images that contravenes the Laws, including the UAE Cybercrimes Law and the UAE Copyright Law (Law No. 38 of 2021), notably: *The "use of information network, electronic information system or information technology methods, for the purpose of breaching the privacy of a person or private or family life of individuals without consent, other than legally permitted, shall be sentenced to detention for a period of not less than (6) six months and/or to pay a fine of not less than (150,000) one hundred fifty thousand Dirhams and not more than (500,000) five hundred thousand Dirhams". This includes "Taking photographs of others at any public or private place or preparing, communicating, exposing, copying or keeping electronic images thereof".* Article 44 of the UAE Cyber Crime Law.
  It is not "permissible for anyone with whom it has been agreed to take a photograph of another or sound or visual recording, in any way whatsoever, to keep, publish, exhibit, or distribute the original or Reproductions thereof without the permission of that person, unless otherwise agreed upon". Article 45 of the UAE Copyright Law.
- Behave in a healthy and positive manner towards digital technologies when engaging in online activities.
- Read and respect (or ask for advice and permission as appropriate) the Terms and Conditions of Web Services (for example - Google Terms and Conditions), especially with regard to the minimum age that some companies set for their websites in order to protect young people from risk.
- Students are able to explain what "Cyberbullying" is and can spot incidents whether they are relating to themself or others.
- Students are aware of the 'go to' people within the school and are encouraged to report any cyberbullying they experience: Classroom Teacher/Form Tutor; Counsellor; Senior leaders; DSL.
- Sign the BYOD Acceptable Use Policy and understand what the agreement means.

Reporting Process for Teachers - all should be reported as soon as possible and as a maximum timeframe, within 24 hours.

- Report anything unusual or inappropriate when teaching lessons. If the issue is related to behaviour, record it on ISAMS (primary) or ClassCharts (secondary); if the behaviour is related to safeguarding, it should be logged on CPOMS.

- Report anything unusual or inappropriate to the IT Team if when accessing their computer, any obscene or inappropriate pop ups, cookies or inadvertent access to inappropriate websites occurs
- If approached by a student or parent/carer with concerns about inappropriate content or misconduct on school social media, staff must log the incident on CPOMS following safeguarding procedures.

Reporting Process for Students - all should be reported as soon as possible and as a maximum timeframe, within 48 hours.

- Report anything unusual or inappropriate during teaching lessons, either in person or online, to the class teacher or form tutor or another trusted adult within the school
- Report to class teacher or form tutor or another trusted adult within the school
  - If/when accessing the device or computer, the student sees any obscene or inappropriate pop ups, cookies or accidentally gains access to inappropriate websites.
- Inform the IT team of any unauthorised use of their password or username of which they become aware as soon as possible.
- Primary students are encouraged to tell a trusted adult if the students see anything that makes them uncomfortable or scared when online using their school online account

BYOD (Bring Your Own Device)

Whilst on site, access to the school network and the internet should be considered a privilege, not a right, and can be suspended immediately, without notice. Access on site is available only for educational and administrative purposes. Digital resources are to be used in accordance with this policy and all users will be required to comply with its regulations.

The purpose of the 'BYOD Acceptable Use' Agreement is to ensure that all students use technology in school, at home and elsewhere, effectively, safely and responsibly, to facilitate learning on a 24/7 basis and to help ensure that they develop the attributes of competent digital citizens.

Device Guidelines

BYOD is strictly limited to laptops, tablets and iPads. Mobile phones are not an acceptable form of BYOD (please refer to Mobile Phone Policy for rules regarding the use of these). We are not particular with the brand or size but the device needs to be suitable for working on, so would recommend a screen that is 11 inches or bigger. A touch screen and digital pen are also recommended. Students must have a Microsoft package downloaded onto the device. Students should bring a charger daily and keep it charged throughout the day.

Device Violations

RIS has a policy related to the use of mobile phones. Please refer to that policy regarding usage. Any activity that goes against this policy may result in a denial of access and possible further disciplinary action. Consequences may include, but are not limited to, notification to parents, suspension of network, technology, or computer privileges, detention or suspension

from school and school-related activities. Students are at risk of legal action and/or prosecution if in violation of any UAE laws.

Use of AI

We recognise that AI is a fast-moving technological development that has the capability to enhance education, support students and teachers, and create an inclusive learning environment. We encourage the use of AI where applicable, for research purposes for example. Our school abides by the JCQ AI Use in Assessments Policy (https://www.jcq.org.uk/exams-office/malpractice/artificial-intelligence/), and any students misusing AI in their assessed work may result in their work being marked as 0. Students assessed work will be checked for plagiarism and AI content using appropriate software. Students are prohibited from using AI to create and/or distribute content that is discriminatory, harmful or offensive. Students who do not use AI tools responsibly may be subject to sanctions, either at an internal school level or externally.

- **Educational Use Only**: AI tools and platforms must only be used to support educational objectives, enhance learning experiences, or improve operational efficiency. Any use beyond this must receive prior approval from the school's leadership team.
- **Data Privacy and Security**: Staff and students must not input any sensitive, personal, or confidential information (e.g., student data, staff details, or school records) into AI systems in order to protect privacy and comply with local regulations.
- **Content Verification**: Any output generated by AI systems must be critically evaluated for accuracy and appropriateness. Staff and students must not rely solely on AI-generated content for decision-making or educational materials.
- **Prohibition of Misuse**: The use of AI tools to create inappropriate, harmful, or misleading content (e.g., deepfakes, offensive material, or misinformation) is strictly prohibited and will result in disciplinary action.
- **Training and Awareness**: The school will provide regular training to ensure all staff and students are aware of the ethical, practical, and legal considerations of using AI responsibly, fostering a culture of informed and safe usage.

Other Related Policies

This policy should be read alongside the following policies, all of which serve to safeguard the children, staff, and parents at Raffles International School:

- RIS Anti-bullying policy
- RIS Behaviour for Learning policy
- RIS Health and Safety Policy
- RIS Safeguarding and Child Protection policy
- RIS Mental Health and Wellbeing Policy
- RIS Mobile Phone Policy

Additional resources

BBC- information for students, staff, and parents regarding staying safe online.
https://www.bbc.com/ownit

Common Sense Media- ratings and reviews of movies, TV series, books, games, apps and podcasts to support parents in making choices for their children.
https://www.commonsensemedia.org

Get Safe Online- internet safety website, with guidance on protecting yourself, children, and your computer.
https://www.getsafeonline.org

Safer Internet Centre- guidance on staying safe online.
https://saferinternet.org.uk

UAE Government Portal- Cyber safety and digital security are serious issues in the UAE. Read how the UAE is protecting its citizens and residents in this field and reinforcing trust in the digital space.
https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security

NSPCC- guidance from the National Society for the Prevention of Cruelty to Children.
https://www.nspcc.org.uk/keeping-children-safe/online-safety/

Internet Matters- lots of guidance and support around supporting online safety.
https://www.internetmatters.org

Policy monitoring and review

Due to the ever-changing nature of digital technology, this policy will be reviewed regularly throughout the academic year. Any changes will be shared immediately.

Appendix 1 - BYOD Acceptable Use Agreement 2025-2026

Please read and sign the BYOD Acceptable Use Agreement between teachers, parents, and students. No student will be permitted to use their own devices unless the agreement is signed by parents and student.

Agreement

Students and parents participating in **Bring Your Own Device** (BYOD) must adhere to the policy.

1. Students take full responsibility for their own devices. RIS is not responsible for the security or transportation of personal devices.
2. Members of staff may access a students device at any time if they believe the device is being misused, or going against anything mentioned in this policy.
3. Devices should not be used during assessments, unless otherwise directed by a teacher.
4. Students may only use devices when in lessons and directed to do so by the teacher.
5. Students must immediately comply with any teacher requests to shut down a device or close the screen. Devices must be in silent mode and put away when asked by teachers.
6. Phones and messenger/WhatsApp on iPads or laptops are not used at school at any time, unless explicit permission has been given.
7. Students are not permitted to capture, transmit or post photographic images/videos of any person on campus for personal reasons or to be posted on public and/or social networking sites.
8. Students should make every effort to charge devices prior to bringing them to school. Students can also bring in chargers if needed. Please label both pieces of equipment.
9. To ensure appropriate network filters, students will only use the wireless connection in school and will not attempt to bypass the network restrictions by using 3G/4G/5G network.
10. Infecting the network with a Virus, Trojan, or program designed to damage, alter, destroy, or provide access to unauthorized data or information is in violation of the policy and will result in severe disciplinary actions. The school maintains the right to collect and examine any device that is suspected of causing problems or is the source of an attack or virus infection.
11. Processing or accessing information on school property related to “hacking,” altering, or bypassing network security policies is in violation of this policy. Students can only access files on the computer or internet sites which are deemed relevant to their learning.
12. Students must adhere to school rules regarding cyberbullying, digital citizenship and netiquette at all times.
13. Students must use their devices in accordance with the Behaviour for Learning policy.
14. Parental guidance and recommendations regarding the suitability of devices can be provided on request from the ICT and Computing Department or Reception.
15. Students, parents, and staff members agree to follow all guidelines and responsibilities within this Digital Safeguarding Policy.

I have read, understand and will abide by the above policy and guidelines. **I understand that any violation will result in the loss of my technology privileges as well as other disciplinary action.**

Full name of Student ……Form class ……. Date ……

Signature of Student ……..

Signature of Parent ……..

Link to Microsoft Form for electronic signature:

https://forms.office.com/r/p5weTur5u6