School Vision	School Mission
Become an institution of innovative education for a society of knowledge and global pioneering.	To equip its graduates with 21st century skills and a high awareness of themselves, their community and the world. It works to ensure they have the ability to make the right decisions, are actively responsible and have essential world-class skills that allow them to pursue their academic and professional goals.

مدرسة رويال الأمريكية
ROYAL AMERICAN SCHOOL

BOYD – Bring your own device

Academic Year

2025-2026

Review date July 2025

This policy has been read and adopted by the Royal American School Board of Trustees and Principal: On behalf of the Board of Trustees, Mr. Mussabah Al Kaabi Chairman of The Board of Trustees and Maritza Vorster School Principal

---

Aim and Purpose:

To regulate the behavior of students when they are using all forms of electronic devices and internet connections on school campus and off school campus when it is directly and/or indirectly related or linked to any other student, teacher, parent, the school and/or other staff member at RAS. This policy will also define the roles and responsibilities of individuals who are involved in all E-safety matters in school.

RAS will deal with any E-safety incidents and associated behavior as per the behavior and anti-bullying policies and will, where known, inform parents/caregivers of incidents of inappropriate e-safety behavior that take place in or out of school.

Roles and Responsibilities

This policy applies to all members of the school including staff, students, parents/caregivers and visitors who have access to and are users of school internet connections and devices. The roles and responsibilities are defined for each group as follows:

IT Systems and Network Administrator

- The school internet access must include effective and efficient filtering appropriate for all age groups.
- The ICT system's capacity and security will be reviewed regularly.
- Virus protection is installed and updated regularly.
- Only approved websites will be accessible.
- All forms of online activities in the school are regularly monitored and any detected misuse is to be communicated to the SLT.

Senior Leadership Team (SLT):

- SLT members are responsible for the approval of the e-policy and for reviewing the contents and the effectiveness of the policy.
- Conduct regular meetings with the health and safety team, teacher, and parents to discuss the online safety -policy.
- Regularly monitor e-safety
- The SLT should ensure that all relevant staff members receive suitable training to enable them to carry out their e-safety roles.

All staff members:

1.All staff members must be fully aware of the contents of this policy and refer to it regularly

- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.
- All staff may only use approved school e-mail accounts for school E-communication**.**

2.Teachers and Teaching Assistants:

- Students will be taught the essentials of internet safety via advisory time, assemblies, campaigns and ICT lessons.
- Students will be educated in the effective use of the Internet in research, including the skills of information location, retrieval, and evaluation.
- Teachers should ensure that the use of internet-derived materials by teachers and students complies with plagiarism and copyright laws.
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Any suspected misuse must be reported to the SLT
- Teachers and TAs will monitor the use of devices and device cameras in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- Teachers are aware that all searches and online activity will be closely monitored by the school.
- When planning lessons, teachers should check that all websites/links/videos are suitable and are culturally and age appropriate for student use.
- When using YouTube links in lessons, teachers must follow the below steps:
    1. Copy the YouTube link chosen for the lesson
    2. Go to the following link: https://video.link/
    3. Copy in the YouTube link to generate the Video link box
    4. Copy the safe URL and use it on plans and PowerPoint presentations.

3.Designated Safeguarding Lead and Deputy Leads**:**

Should be trained in all e-safety matters 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 online contact with adults/strangers.
• Potential or actual incidents of grooming.

• Cyber-bullying.

Students:

- Students are mindful that network and internet use is monitored.
- Must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.
- Are responsible for using their devices in an appropriate manner. This includes their use of digital cameras.
- Have a good understanding of research skills and the need to avoid plagiarism and respect copyright laws.
- Must report any abuse, misuse, or access to inappropriate materials to their teacher, SLT or to a member of the health and safety team and/or the safeguarding team.
- Must not leave their devices unattended as the school is not responsible for missing/ damaged devices.

Parents/Caregivers:

Parents/Caregivers play a crucial role in ensuring that their children understand the importance of E-safety practices both in and out of school. The school will take every opportunity to help parents understand these issues through parents' coffee mornings, newsletters, and sharing of school policies. Parents/caregivers roles and responsibilities include:

- Reading and discussing this E-policy with their children.
- Monitor their children's activity on their devices at home.
- Report any cases of misuse and/or cyberbullying targeting any member of the school. Community to a member of the Senior Leadership Team or Health and Safety Team.

-

Policy Statements

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling e-safety complaints

- Complaints of internet misuse will be dealt with by the SLT team and the appropriate departments
- Any complaint about staff misuse must be referred to the school Principal.

- Complaints of a child protection nature must be dealt with in accordance with the safeguarding policy and handled by the Safeguarding team.
- Students and parents will be informed of who they can approach to make complaints regarding e-safety via assemblies, advisory time, newsletters, and school campaigns.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones are strictly forbidden in the school.
- Sending abusive or inappropriate text messages and/or other forms of online messaging/posts will be dealt with in accordance with the RAS behavior policy.

E -policy Communication with Parents:

- Parents' attention will be drawn to the School e-Safety Policy during the various informational coffee mornings, newsletters, and handbook.
- Parents will, from time to time, be provided with additional information on e-safety.

Cyberbullying

All students are made aware of the impact of cyberbullying and the ways it differs from other bullying - including the risks of misinterpretation of comments posted. This is communicated to students through assemblies, constant reminders by teachers, and internet safety campaigns.

- RAS takes all reasonable steps to block access to unsuitable internet sites, including social networking sites, chat rooms, and individual website owners/forums and message board hosts.

- RAS is able to conduct a search of internet use records and act accordingly to stop misuse of school equipment and systems.

- Staff are required to keep a record of all bullying cases as evidence and the police can be involved, when needed, to enable the service provider to look into the data of another user.

- Students are made aware that some cyberbullying activities could be criminal offenses. Internet Safety Day is celebrated and campaigns are held to create awareness for both students and parents.

- RAS reinforces statutory guidelines about the use of social network sites e.g. Facebook, Twitter, Instagram and Snapchat.

Online safety – Extract from the RAS Safeguarding Manual

The school provides internet and intranet access to students and staff as well as access to other online platforms. Students and staff must comply with the respective Acceptable Use of Technology Policy when using School Technology. All such use is monitored by the IT Manager and his/her team.
Students and staff require individual usernames and passwords to access the school's internet and intranet sites and email system, which must not be disclosed to any other person. Any student or member of staff who has a problem with their usernames or passwords must report it to the IT Department immediately.

No laptop, tablet or other mobile electronic device may be connected to the school network without the consent of the IT Manager. All devices connected to the school's network should have current and up- to-date anti-virus software installed and have the latest OS updates applied. The use of any device connected to the school's network will be logged in and monitored by the IT Support Department.

The school has a separate Wi-Fi connection available for use by visitors to the school. A password, which is changed on a regular basis, must be obtained from a member of staff in order to use the Wi-Fi. Use of this service will be logged and monitored by the IT Department.

All incidents of youth produced sexual imagery (YPSI) will be dealt with as safeguarding concerns. The primary concern at all times will be the welfare and protection of the young people involved. Students who share sexual imagery of themselves or their peers are breaking the law. However, the school believes it is important to avoid criminalizing young people unnecessarily. The school will work in partnership with parents and external agencies with a view to responding proportionately to the circumstances of any incident.

All incidents of YPSI must be reported to the DSL as with all other safeguarding issues and concerns. Staff will not make their own judgements about whether an issue relating to YPSI is more or less serious enough to warrant a report to the DSL. If, at any point in the process, there is concern that a young person has been harmed or is at risk of harm, a referral will be made to the relevant agency.

Important points to note:

Students and parents should be aware that devices are subject to search by school administrators if the device is suspected of a violation of the student code of conduct or this agreement. If the device is locked or password protected, the student will be required to unlock the device at the request of a school administrator. Parental permission will be requested before this is done.

Lost, Stolen, or Damaged Devices:

Each user is responsible for his/her own device and should use it responsibly and appropriately. RAS takes no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices. While school employees will help students identify how to keep personal devices secure, students will have the final responsibility for securing their personal devices.

Usage Charges:

RAS is not responsible for any possible device charges to your account that might be incurred during approved school-related use.

I understand and will abide by the above policy and guidelines. I further understand that any violation is unethical and may result in the loss of my network and/or device privileges as well as other disciplinary actions. During the school year, additional rules regarding personal device use may be added.

Mobile Phone Confiscation Policy

In order to maintain a focused and distraction-free learning environment, and to ensure students' adherence to school rules and discipline, Royal American School implements the following policy regarding the use of mobile phones on school premises:

First Offense:

- The student's mobile phone will be confiscated**.**
- The phone will be returned at the end of the school day**.**

Second Offense:

- The phone will be **confiscated**.
- It will only be **returned after one week** from the date of confiscation.
- The phone will be handed over **in person to the parent at the school**.
- The parent will be required to **sign a written commitment not to allow the student to bring a phone to school again**.

Third Offense:

- The phone will be **confiscated until the end of the term**.
- It will only be **returned in person to the parent**.
- The parent will be required to **sign a final commitment not to allow the student to bring a phone to school for the remainder of the term**.

IPads and Laptops

- **Students are not allowed to bring iPads, laptops, or similar electronic devices** to school **unless specifically requested by the school** for educational purposes.
- **If a student brings such devices without prior school authorization**, the **same confiscation policy as for mobile phones will apply**, including written commitments and escalating consequences.

Unauthorized Photography, Recording, or Content Sharing

If a student **photographs, records (audio or video), publishes, distributes, or shares** any content involving **the school premises, students, staff, classrooms, or school events—without prior written permission from school administration**—this will be considered a **serious violation** of the school's policies related to privacy, safety, and digital conduct.

This includes, but is not limited to:

- Taking photos or videos of students, teachers, or school staff without consent.
- Recording inside classrooms or during school activities without permission.
- Sharing any media captured at school on social media platforms, messaging apps, or any other digital medium.
- Assisting or encouraging others to commit any of the above actions.

Such actions may:

- Violate the privacy of individuals.
- Cause reputational harm to students, staff, or the school.
- Disrupt the learning environment.
- Breach national laws and regulations on data protection or cybercrime (where applicable
- The consequences will be applied in accordance with the severity level stated in the School Behavior Policy.

Smartwatches Policy

Smartwatches are **strictly prohibited** on school premises.

These devices are considered a form of personal communication and recording tool, and therefore, **the same confiscation policy that applies to mobile phones will also apply to smartwatches**.

If a student is found wearing or using a smartwatch during school hours:

- The device will be **confiscated immediately**.
- **Consequences will follow the same steps outlined for mobile phone violations**, including parental notification, written commitments, and progressive disciplinary action.

Disclaimer Regarding Electronic Devices

Please note that **the school is not responsible for the loss, theft, or damage of any personal electronic device** (including but not limited to mobile phones, iPads, laptops, smartwatches, headphones, etc.) brought onto school premises **with or without permission**.

Students and parents are strongly advised to avoid bringing valuable devices to school unless explicitly requested by the administration. Any device brought at the student's own risk will remain **solely under their responsibility**.

We kindly ask all students and parents to adhere to this policy in the best interest of maintaining discipline and supporting the educational environment at the school.

Royal American School Administration