POLICY ON THE USE OF DIGITAL DEVICES, THE INTERNET AND SOCIAL MEDIA

How do we ensure the safety and well-being of our students at school? Measures related to DIGITAL SAFETY.

5th Revision: July 2025

TABLE OF CONTENTS

1.- POLICY OBJECTIVES

Like all social phenomena, education has been impacted in recent years by the rapid and growing digitalisation, so it is appropriate for the school to establish an optimal framework for coexistence and behaviour that responds to the excellence of the students at Internacional Aravaca.

Internacional Aravaca recognises that information and communications are essential for participation in today's society, as is the demand from students for interactivity in learning, communication and entertainment. In this regard, Internacional Aravaca students stand out as capable, innovative, creative and productive users of new technologies, which is why the school will become a large learning community with even greater collaboration between students, teachers, families and the community at large.

To achieve this, the school provides its students with tools such as the iPad, which will enhance this new experience.
These regulations aim to ensure:

- That teachers and students make responsible and safe use of the Internet and other communication technologies for educational and personal purposes.
- That the school's Information and Communication Technology (ICT) systems and users will be monitored for any misuse or intentional use that could jeopardise the security of the systems and users.

2.- INTERNET AT SCHOOL

Internet access at school

The Internet and other digital information and communication technologies are powerful tools that offer many possibilities for everyone. These technologies can encourage debate, promote creativity and stimulate awareness of the context for effective learning. They also offer teachers the opportunity to be more creative and productive at work.

The term "mobile device" in these regulations refers to mobile phones, laptops, iPod touches, tablets such as iPads, smartwatches, Android devices or any other mobile device that can connect to the Internacional Aracaca network.

Appropriate and safe access to the Internet

As with other media such as magazines, books, or videos, there is content on the Internet that is not

suitable for students. The school will take measures to ensure that students do not encounter disturbing, offensive, or inappropriate content on the Internet. (MDM+Firewall)

In order to ensure that our students are not exposed to inappropriate material and know how to act, the following measures are published:

- Internet access has a filtering system configured at the centre, which prevents access to material that is inappropriate for minors.
- Students who use the Internet will do so safely under the MDM filters and security systems at the Centre.
- To safeguard students and teachers through the school's devices, we have a new filtering system called Smoothwall, which allows us to monitor alerts for misuse of the device through key terms. We can also take action if we detect dangerous terms or terms that could threaten the safety of students, teachers or classmates.
- Teachers will use their own professional judgement and check that the websites selected for use by students are appropriate for their age and level of maturity.
- With some exceptions, iPads in primary school will only go home one afternoon a week and on weekends, and always under limited instructions and activities related to research or the use of specific platforms. On all other days, the iPad will remain at school.
- Teachers will encourage students to be aware that information must be verified before it can be taken as true and that the need to verify is even more important when the information comes from the Internet.

Maintaining the security of the school's computer network

Maintaining the school's computer network is the responsibility of the IT department, which oversees the proper functioning of our equipment and systems, as well as their security.

- Students will be educated to be responsible in their use of the Internet through information sessions and practical classes on 'Internet safety' for families and students at the school.
- Students will know that they must turn off the screen and immediately report to an adult if they encounter any content that makes them feel uncomfortable. In such a situation, the tutor and the school will take immediate action.
- When copying content from the web, students will be taught to respect copyright conditions.
- Students will be made aware of the possibility that the identity of someone writing by email may not be who they say they are.

3.- CONSIDERATIONS TO BE TAKEN INTO ACCOUNT

1. All devices at the School, including iPads, are tools for students' academic development. They are solely and exclusively tools for learning and studying, not for entertainment, linked to classroom activities and access to information resources derived from exercises, projects and school assignments, and under the guidance and supervision of the teacher and technical team for the academic development of students. Studying with a device does not exclude the use of other media and tools. The use of notebooks and other resources is mandatory in all subjects.
2. The student is solely responsible for the iPad.
3. In the event of any conflict between academic and personal use of the device, academic use shall prevail.
4. Educational uses and purposes will be linked to classroom activities and access to information resources derived from school assignments.
5. The instructions of the teacher and technical team will set the guidelines for working with the devices.
6. The Centre is not responsible for configuring access to networks other than those belonging to the School (home networks, public networks, private Internet access, etc.).

4.- GENERAL CONDITIONS

1. The Centre reserves the right to decide which applications are prohibited. The installation of non-educational applications or games will therefore be supervised by the school. An MDM (Mobile Device Management) system will be installed on each device to ensure that teachers and parents can control the tool. It is not permitted to exit this system.
2. At school, pupils are prohibited from using any device to access inappropriate websites, social networks, download, distribute, store or display offensive material that is discriminatory or could offend others, distribute defamatory, obscene, offensive or harassing messages, or participate in any illegal or illicit activity.
3. At school, students are required to hand over and show any work device to the teacher or technical staff whenever they deem it appropriate and request it in order to check and supervise the suitability of the content and the correct use of the device.
4. Cameras and video cameras may only be used when required for a project and with the authorisation of a school teacher. Under no circumstances is it permitted to take photographs or make video recordings in which other students or teachers appear without their explicit consent, unless instructed to do so by the teacher or for exclusively academic purposes.

5. Impersonation or hacking of one's own or others' devices, as well as access to a classmate's iPad or accounts, is not permitted. The iPad and its resources are for personal use and are non-transferable.
6. Removing or modifying the original Apple operating system is not permitted, except for system updates or apps, which are the only exceptions to this rule.

5.- STUDENT DUTIES AND OBLIGATIONS

1. Students are responsible for the cleanliness and maintenance of their device, as well as any technical tools made available to them by the School.
2. Students are responsible for bringing their iPad to school fully charged every day and must bring their iPad to school every school day unless otherwise specified by the school.
3. It is the student's responsibility to store personal and academic content appropriately.
4. Students are responsible for keeping track of their iPads, and the school provides personal lockers in the classrooms for each student.
5. Outside the classroom and areas designated for activities, projects and tasks, particularly in the entrance hall, playgrounds, changing rooms and dining hall, etc., students must refrain from using devices, unless expressly authorised by the teacher.
6. Students are required to report any damage to the device to the school.
7. When leaving school, the iPad must be properly stored in the backpack, not exposed to the outside.
8. Students are responsible for maintaining the initial configuration of the device. If this configuration is altered due to misuse and has to be reset to its initial configuration, the cost of doing so will be assessed.
9. During outings, excursions and special activities, the device may not be taken, unless expressly authorised, in which case the student has the duty to keep their mobile phone switched off and stored away, especially in places where its use is not permitted: cinemas, theatres, museums, meetings, hospitals, as well as any place where it is required to be kept switched off, unless expressly authorised by the teacher in charge or the coordinator.
10. Students must also understand when and/or where it is inappropriate to use a mobile phone. In particular, students are prohibited from using their mobile phones at school and in the classroom. If they have to bring the device to school, they must hand it in to the school office at the beginning of the school day and collect it before leaving. Under no circumstances may they have the device in class or use it within the school premises. Specifically, the use of mobile phones by students at school without authorisation is classified as a serious offence and the school may confiscate the student's mobile phone until it is deemed appropriate, after speaking with the families involved.
11. The school will never be responsible for technical objects or mobile devices that students bring to school. This includes pencils, headphones, or mobile phones.

12. Students have a duty to think before writing, publishing, and sharing anything online, and are obliged to bear in mind aspects such as the importance, significance, and multiplied and uncontrolled dissemination that published or shared information may have.

6.- ACCOUNTS: GOOGLE AND APPLE

At school, and with the explicit consent of families, we use Google Education resources as a means of communication with various digital platforms. Email, among other tools, is part of our daily routine. From Year 4 onwards, pupils have an iPad device where this Google account plays an important role in classroom workflow, work and communication. Likewise, for purely technical purposes, pupils will have an Apple ID managed by the school.

In this regard, we expect the following from students and families:

1. These accounts will be used exclusively for academic purposes, as they are a work tool for the student.
2. The access codes and passwords are for the exclusive, private and confidential use of the student who owns them, and therefore their correct use and safekeeping are their responsibility, and their use by third parties is prohibited.
3. Both Google services and Apple ID are free of charge.
4. The user shall have the right to use the accounts while they are a student at the Centre, and this right shall be withdrawn when they cease to be a student at the school.

With regard to these accounts, the School:

1. Aravaca International School reserves the right to totally or partially deprive the user of the rights to use the accounts if misuse or use other than for the purpose of the account is detected.
2. Aravaca International School will apply the restrictions it deems appropriate to Google and Apple ID accounts to ensure proper educational use. This includes restrictions on sending and receiving external emails, or restrictions on the use of Google applications.
3. Colegio Internacional Aravaca shall be exempt from any liability for damages that may arise from the content of electronic messages managed through this service, as well as from the misuse of Apple ID or the use of any application or programme derived from them.
4. Colegio Internacional Aravaca may exercise control, supervision and audits when it deems necessary on the use and content of the accounts.
5. Aravaca International School guarantees that it will not collect information from the contents of users' messages once their stay at the school has ended, nor from the information stored in the Apple account.
6. Colegio Internacional Aravaca warns that Article 197 of the Spanish Penal Code punishes anyone who takes possession of another person's e-mail messages without their consent with imprisonment for one to four years.

7.- SECURITY

The safety and security of our students is one of the cornerstones of Aravaca International School. In the daily use of technology, it is important to maintain standards and criteria that help us to achieve this goal.

1. Students have a duty to act with absolute caution, prudence and critical thinking when participating in *online* games and sweepstakes, opening emails from abroad whose address arouses suspicion; participating in surveys and invitations that appear to be free for messaging services and similar services; and they also have a duty to avoid websites that ask for money, credit card numbers or personal information, while also learning how to configure the privacy options offered by these services to determine what information can be accessed by other people.
2. Students have a duty not to visit unreliable websites, as well as a duty to be wary of strange messages they may receive through social networks and other services, especially if these messages include links to other content and particularly if they ask for personal data to be entered into dubious or suspicious forms. In this regard, it is even advisable to be wary of messages from known contacts, as these contacts may be infected with *malware or* malicious software.
3. At school, pupils are prohibited from chatting, sending or checking messages, playing and watching videos, downloading music, commenting on blogs or forums, playing or participating in online games, accessing social media, participating in competitions, creating events, contracting services or purchasing products online, etc., unless authorised and supervised by the responsible teacher as part of a class activity in the relevant context.
4. When registering on websites to participate in prize draws, receive news, enter forums and other similar actions, students have a duty to be aware of the need to pay special attention to where and to whom they send personal data. In these cases, before sending such data, students must carefully read the website's terms of use and privacy policy in order to understand what these websites may do with such data, and always with the prior authorisation and permission of their parents.
5. Whenever forwarding emails, students have a duty to first delete any previous addresses that appear in the message, as they must protect other people's email addresses. Likewise, and for the same purpose, they must take the precaution, when appropriate, of writing addresses with blind carbon copy (BCC).
6. At school, students have a duty to hand over and show their device to the teacher whenever the teacher deems it appropriate and requests it in order to check and supervise the suitability of the content and the correct use of the device.
7. Students have a duty to avoid using the corporate image, uniform, symbols, emblems and logos of Internacional Aravaca in their publications and personal social media accounts without the express authorisation of the Headteacher.

8. Students must limit their use of images and content related to Internacional Aravaca to the school's official accounts and websites. Students must therefore act correctly and cautiously when publishing photographs and images wearing the school uniform. In this regard, Internacional Aravaca reserves the right to demand the removal from the internet of images or content related to the school and published without the consent or permission of the Headteacher.
9. Students have a duty to be aware of and accept that the law prohibits the destruction, alteration, disabling or damage of data, programmes or electronic documents belonging to others contained in networks, media or computer systems.

8.- MOBILE DEVICES - mobile phones and smartwatches

8.1 BASIC PRINCIPLES

The well-being and comprehensive development of our students are our top priority. In order to ensure a safe and distraction-free learning environment, the following rules regarding the use of mobile phones on school grounds have been established. This policy is based on current educational legislation in the United Kingdom and the school's internal regulations. It is also in line with recommendations from organisations such as UNESCO and the World Health Organisation, which warn of the negative impact of excessive use of digital devices on minors, affecting their cognitive and social development, reducing attention span, increasing anxiety and affecting academic performance.

8.2 REGULATIONS

Students **are prohibited from using personal mobile devices on school premises** during the school day, which includes class time, breaks, complementary and extracurricular activities, as well as when entering and leaving the school. This includes smartwatches.

If parents wish to communicate with their children during the school day, they may do so by calling the school office, which will relay the message to the student in an appropriate manner. This ensures an effective channel of communication without affecting the educational environment.

Please note: If a pupil needs to bring their mobile phone to school, they must hand it in to the school office on arrival and collect it at the end of the school day.

8.3 EXCEPTIONS

Exceptions to this policy will be evaluated and authorised only by the school management in specific circumstances. There are two specific situations in which the use of mobile phones within the school may be authorised:

1. **Medical reasons:** Parents or guardians may request authorisation for their child to bring a mobile phone in the event of a documented medical need. To do so, they must submit a written request along with the relevant medical documentation. The school management will evaluate the request and, if approved, clear conditions for its use will be established.

2. **Specific educational projects:** For certain educational activities, the school may authorise the use of mobile phones for specific projects. In these cases, the school will inform families in advance, specifying the periods and conditions of use. However, the use of mobile phones will never be compulsory or essential for the activity, and parents may decide not to send the device to school if they wish.

3. On **field trips and school camps**, the specific guidelines deemed appropriate by the school will be followed, and families will be informed of these measures.

8.4 RESPONSIBILITY AND SAFETY

The school **is not responsible for the loss, theft or damage of mobile phones** brought by students **under any circumstances**, even if they have been authorised to bring them to the school. It is strongly recommended that students do not bring these devices to school to avoid any inconvenience. Likewise, any inappropriate use of the device inside or outside the school will be the sole responsibility of the student and their family. However, if the device is lost, the student must immediately notify the teaching staff.

8.5 MISUSE OF THE DEVICE AND CONSEQUENCES

- If a student uses their mobile device at school, they will receive the appropriate sanction in accordance with the coexistence plan and their parents will be informed immediately. This is considered **a serious offence** with the following consequences: confiscation of the mobile phone (the SIM card will be returned) or a two-day suspension from school (to be agreed with the family). If the offence is repeated, the accumulation of offences governed by our coexistence plan and its consequences will apply. LINK
- **Taking photographs or recordings** without the consent of other students, teachers or school staff may constitute a violation of the right to privacy and data protection regulations. In the event of such conduct, **the school will not be held responsible for any legal implications that may arise in the event** of a claim by the affected person, this being the sole responsibility of the student and their family.

Additionally, it should be noted that when misuse of the device involves an additional breach of the school's Code of Conduct, such as the use of images or recordings to **intimidate, harass or bully,** additional penalties may also be imposed in accordance with the school's disciplinary regulations, which may include more severe measures depending on the seriousness of the offence. It is equally important to note that these actions may have criminal consequences.

8.6 TEACHING STAFF

Teachers and staff at the centre should avoid using personal devices as much as possible, especially during classes or when supervising playgrounds or the dining hall.

Photographs of educational activities, events and excursions must always be taken using the devices provided for this purpose by the school or the marketing department. If a personal device has to be used for this purpose, the photographs or videos must be uploaded to the corresponding Google Drive folder and deleted from the device as soon as possible.

Teachers communicate with students through the platforms designated for this purpose: email, Google Classroom, etc. Under no circumstances should they give their personal number to students.

8.7. AWARENESS AND TRAINING

The school will carry out awareness programmes aimed at students, families and educational staff on the responsible and safe use of digital technologies, promoting a culture of respect and responsibility in the digital environment. Information will be provided on cybersecurity, technology addiction and the risks of unsupervised use of mobile devices.

9.- ONLINE BEHAVIOUR

CYBERBULLYING

Cyberbullying or bullying via the internet is defined as the use and dissemination of information, whether real or fictitious, with the intention of causing harm or defamation, in electronic format.

This dissemination can be carried out through various digital communication media such as email, instant messaging, forums, chats, social networks, text messaging via mobile devices or the publication of videos or photographs on electronic content dissemination platforms.

This form of harassment or bullying can manifest itself in many different ways.

In this regard:

1. Students have a duty to maintain a behaviour and attitude of absolute vigilance and responsibility in the defence and protection of their personal data and that of their classmates, and in this regard, they have an obligation to consult with parents and teachers and to understand and configure in detail the privacy options of the various instant messaging and social media services.
2. Students have a duty not to engage in cyberbullying behaviour and, if they are affected by this type of behaviour or are aware of such acts or conduct, they must report it immediately to their teachers or the relevant coordinator.
3. Students have a duty to report and not to condone acts of psychological or moral violence against other students on social media, chats, messaging services, forums, etc., from the moment they become aware of them.
4. Students have a duty to avoid at all times making jokes about behaviour that could be defined as harassment and cyberbullying, and must behave with responsible caution in this regard.
5. Students have a duty to avoid intimidation, deception, mockery and ridicule, rejection and all forms of discrimination, exclusion and/or harassment of other students with offensive comments in forums, chats, social networks, etc.
6. Students have a duty to refrain from sending and sharing photographs or images of other classmates with the intention of making fun of them with their friends.

7. Students have a duty not to post comments, photos or videos that could damage the reputation, defame or hurt the feelings of another student.
8. Students must avoid using forums, chats, closed groups or friends lists on social media or instant messaging services as a means of excluding other students with the aim of marginalising or rejecting them.
9. Students have a duty to avoid offensive, threatening or intimidating messages or those containing aggressive and foul language or vocabulary, and must also avoid messages that, directly or indirectly, are insulting or imply harassment, exclusion or manipulation.
10. Students have a duty to avoid spreading or propagating gossip or false rumours of a cruel nature or that seek to damage the reputation of another student.
11. Students have a duty to avoid appropriating and using other people's passwords to falsify and impersonate another student.
12. Students have a duty to refrain from recording intimate content and compromising private images of other students.
13. Students have a duty to avoid disseminating, forwarding or circulating personal data belonging to classmates and/or their families to other students, third parties or people outside the school.
14. Students must not respond to threats, insults, intimidating messages or provocations directed at them via forums, chats, social networks, etc. In such situations, students must always inform their parents, guardians and teachers.

Aggravating circumstances:

15. Threatening to publicise a matter, i.e. in such a way that third parties may become aware of the nature of the intimidation.
16. Threatening to reveal or disseminate facts about the private life or relationships of another student in cases where, if the threat is carried out, the victim's reputation or personal interests may be affected.
17. Coercion: threatening, with violence of any kind, to prevent a student from doing something lawful or in accordance with the rules of coexistence, or to force them to do something they do not want to do, whether or not it is lawful or in accordance with the rules.
18. Blackmail: a threat with a condition, demanding something in exchange for not carrying out the threat.

SLANDER AND INSULTS

Slander is making a false accusation that another student has acted outside or against the rules, knowing that they have never committed any offence against those rules.

Insults are any serious actions or expressions—humiliation, insults, or offences—that damage another student's dignity, undermine their reputation, or attack their self-esteem.

1. In general, on the internet, forums, chats, social networks, instant messaging services, etc., students have a duty to treat other students with respect and avoid comments that may be hurtful.

2. Students have a duty to avoid publicly slandering or insulting other students on the internet, forums, chats, social networks, instant messaging services, etc.

Aggravating circumstances:

3. Slander or insults in exchange for a reward or promise from third parties.
4. The existence of degrading treatment that seriously affects the moral integrity of another student.

10.- VIOLATIONS OF PRIVACY

The violation or infringement of the right to privacy can have legal consequences: the law prohibits accessing, seizing, using, modifying, and altering another individual's personal data and privacy to their detriment.

The secrecy of communications is a fundamental right of individuals and failure to respect it can lead to serious consequences. Email, instant messaging, chat conversations, text messages, social networks, etc. are means of communication and, if used privately, are protected by law.

In this regard, the dissemination, disclosure or transfer of third-party data to third parties without consent, for example, by publishing it on the internet, may have legal repercussions, which are particularly serious if they concern a minor.

With regard to personal privacy, Article 18.4 of the Spanish Constitution guarantees the protection of personal data, so that it cannot be used without the informed consent of the data subject and for specific purposes.
It is extremely important that students are aware of the extent to which their behaviour may or may not be appropriate and, above all, that they understand and appreciate the importance of respecting the privacy of others and the possible consequences of acting contrary to this.

1. When recording and/or publishing images and photographs in which other students appear, students have a duty to do so with their consent and permission.
2. Students have a duty to refrain from uploading, posting or linking to any document or image – photographs, videos, web pages, audio files, forums, groups, chats, etc. – that may cause or lead to present or future harm, discredit or damage to the privacy of another student.
3. Students must refrain from reading other students' emails without their permission, as well as accessing their computers or systems without their permission, as this constitutes an invasion of their privacy.

Internacional Aravaca expressly warns that, in accordance with the Penal Code, the violation or breach of any of the above prohibitions constitutes a crime and that in Spain, minors between the ages of 14 and 18

can be tried by special judges and courts and punished for committing a crime. In the case of minors under the age of 14, a financial penalty may be imposed on their parents or guardians, depending on the offence committed.

11.- TRAINING.

The increase in the use of networks, the internet and devices has heightened the dangers and different situations that can arise. In order to advise and train students, families and teachers, the school has an innovation department that specialises in the safety and protection of minors on the internet, as well as ensuring the integrity and protection of students when using the internet.

Throughout the school year, sessions are held with all students on aspects of online safety. We use tutorial time for this purpose, with the help of content provided by the Guidance Department.

Families are offered the opportunity to attend one or more annual online sessions on cybersecurity and the internet for children. These sessions provide updates on current internet content and offer information and tools for working on these issues at home and promoting a safe environment for children in the home.

12.- COMMUNICATION.

We are aware that every day we encounter more and more different situations with our students, generated by the continuous use of the internet inside and outside the classroom, and with personal devices.

The school's innovation department provides families, students and staff with channels to obtain information, ask questions or receive advice on specific issues they may need. The person to contact for the various topics is:

Miguel Asensio (Head of Learning) -m.asensio@ia.edu.es :

- Cybersecurity issues
- Online child protection
- Online safeguarding issues
- Online safety at school
- Use of mobile devices

Marta Martínez (Headmistress) - m.martinez@ia.edu.es

- Issues relating to teaching staff

Miriam Serrano (DSL) - m.serrano@ia.edu.es
- Safeguarding issues
- Security situations

Borja Espresati (IT) -b.espresati@ia.edu.es
- Students' digital licences
- School devices
- School network security
- Email and Google tools
- Technical and security issues
- Digital licences

Marta García (Billing) - m.garcia@ia.edu.es
- Financial aspects of projects

13.- APPENDIX.

How do we work on online safety at the School? Measures implemented related to the security and safeguarding of students on iPads.

Link to the 12 Questions and Answers (FAQs) about security on devices: https://docs.google.com/document/d/11fKCxXSQ1C5aVuFaAxTHjDIoxQj7Gs4zKN6NYc3zqf4/edit?usp=sharing