ALMUÑÉCAR INTERNATIONAL SCHOOL

Policy Acceptable Use of ICT at AIS - Students and Parents - English v10

Reviewed August 2025 by M.Ives

Next review due August 2026
Changes from the previous version are highlighted

Acceptable Use of ICT at AIS
STUDENTS / PARENTS

Introduction

Any use of computer systems, computer equipment or rooms, online subscriptions, AIS social media or administration systems connected with AIS (in school or outside of school premises) either as a visitor or using login details confirms that you have read and understood the AIS Acceptable Use of ICT policy (this document) as well as Student and Parental Promise – Use of Digital Services at AIS and any current policies relating to Use of AIS and for staff - Staff ICT Use.

It is every user's responsibility to ensure that they read updates to this policy. These will be posted on parental Engage homepages and parents informed of this by email.

The overall intention of this document is to create a safe and efficient way of using ICT at AIS. It is not the intention to stop the use of ICT in any way other than for the reason of child protection or for the safety of other users.

This document has been created by reading and using other school´s and government department policies (in the UK and Spain).

This document is to be read and signed alongside the "Student / Parent Promise – use of Digital Services at AIS and associated policies.

The user of AIS ICT will be fully responsible in case of failure to comply with this Policy for any consequences and the disciplinary measures inside or outside of AIS that it may entail. Users also understand that in the case they fail to comply with this policy, AIS and its employees would not be responsible to any extent.

General

Use of on site computers or of any web or communication service that Almunecar International School makes available to students and teachers for use outside school is subject to the same principles and rules which govern behaviour within school. The Code of Conduct that applies in school extends to online activities and behaviour in virtual environments or communication forums provided by the school.

The above general principle applies in all areas of conduct, with special reference to the following.

Personal Relationships

We require the same standards of respect, courtesy and tolerance for fellow students and staff as we do at school.

Any type of bullying, harassment, attempts to embarrass, deceive or manipulate would not be accepted and would be investigated and sanctioned accordingly and proportionately. Users must not attempt to disrupt the work of others in any way, for example by using hacking commands or utilities to turn off machines.

These kinds of actions could entail disciplinary measures according to the seriousness of the offences and actions performed.

The individual who may commit these kinds of actions would be considered as fully responsible for any consequences derived from these, neither AIS or any of its employees will have any responsibility to any extent.

Appropriate Expression

It is prohibited to publish online and or send messages not considered as fully acceptable by the school management. Opinions and comments about other members of the school community and the school itself are subject to the norms that govern school life in general. Any inappropriate and/or offensive comments about other students or members of staff would not be accepted by AIS, entailing the corresponding disciplinary measures. AIS and its employees would not be responsible to any extent for the consequences of those opinions or commentaries made by students/and or parents.

3

Appropriate Content

Racist or pornographic texts or images and similar types of materials would not be tolerable in school, and neither will they online.

Content filters are in place on the student networks that operate in school, but the dynamic nature of the Internet means even the best filters cannot be guaranteed 100% reliable, and in the last resort the responsibility lies with the user: if an inappropriate web page does appear for any reason, it must be reported to staff who will pass on the information to the appropriate person. Please note that the system keeps a time-stamped log of every web page accessed.

Any misuse or inappropriate use of contents will result in the corresponding disciplinary measures.
AIS and its employees would not be responsible to any extent for the consequences of those inappropriate uses made by students / and or any other user.

Respect for Property

The ICT system, software and hardware, is the property of the school and must be treated with the same care as any other valuable installations in school. Users must not attempt / are prohibited to download, install, modify or remove any software, bypass Internet filtering systems, or place the system at risk of viruses through use of contaminated removable media (USB memory sticks, mobile phones, MP3 players etc) which could damage school ICT systems. Downloading, sending or publishing material that violates copyright or data protection law is forbidden, as is copying other users' files without their express permission. Hardware must not be disconnected, adjusted, moved or unplugged without the permission of staff.

Breaching any of these rules could result in corresponding disciplinary measures.
AIS and its employees would not be responsible to any extent for the consequences of the inappropriate use or lack of respect for the school ICT system made by students / and or any other user.

Security and Privacy

Users must not (knowingly) attempt / are forbidden to compromise the security of the system or take any actions that jeopardise the privacy of others. This includes impersonating another user (real or fictional) by logging on with their credentials, attempting to bypass security settings to gain access to restricted or personal files, sending unsolicited material to other users (including those on external networks) are not allowed.

Breaching any of these rules could result in corresponding disciplinary measures.
AIS and its employees would not be responsible to any extent for the consequences of the inappropriate use or lack of respect for the school ICT system made by students / and or any other user.

Appropriate Use of Resources

As with any equipment provided by the school, the ICT services and equipment are exclusively for use in the delivery of the curriculum. Activities that do not relate to this end are only permitted if explicitly authorised by a member of staff as part of a lesson. Activities considered as offensive and others may severely reduce overall system performance. Such activities include (without this list being exclusive):

- personal and social networking
- gaming
- downloading music or video
- streaming audio or video for fun
- shopping, auctioning, etc
- chatting
- uploading photos
- sending or replying to chain or joke emails
- sending emails to mailing lists without good reason
- sending emails with large attachments

SANCTIONS

Infringements of this Policy may lead to any of the sanctions and disciplinary measures described in the Code of Conduct, with the additional option of a ban on the use of ICT facilities.

Parents and Students would be considered as fully responsible for any infringement or disregard of this policy.
AIS and its employees would not be responsible to any extent for the consequences of the infringements performed by students / and or any other user.

e-Safety

ICT systems in school are designed to help ensure students safety online by restricting websites that might be dangerous. However, users are responsible for their own security and for observing the following precautions when working online:

Do Not

- Give personal information such as address or phone number to strangers.
- Tell your login to anyone else.
- Use a "nickname" with your personal name or your age.
- Believe everything you read online.
- Use webcams with strangers.
- Accept "blind dates" (arrange to meet a stranger).
- Post personal photos in public areas.
- Accept or post insults in any form (text, photo or video).
- Answer messages from unknown sources.
- Click on silly adverts or obviously download inappropriate links.

Do

- Tell your parents or staff if anything you have seen or read bothers or disturbs you.
- Limit the amount of time you spend on the internet, chatting, playing games etc.
- Turn on "safe filters" when searching the internet.
- Socialise with real friends not just "virtual" ones.
- Save your work regularly.
- Make a "back up" of your work on another computer or USB pen (on your own device).

Basic Security Rules- for everyone´s benefit

All users of all online services provided by AIS should be aware of basic security when accessing accounts.

Use your own common sense when working with any of the online or school network services at AIS. Remember that yours and other people's data is at risk if you do not use the systems in a secure way.

MAKE SURE that your passwords are complex but memorable - do not use dates of birth, pet names etc. ALWAYS include capitals / lowercase / numerals / punctuation

DO NOT write down or tell anyone your password or username. If you need to write it down it is probably not a memorable or useful password. It is certainly not secure.

ALWAYS make sure that you log out of the service when you have finished using it.

ALWAYS log out of a service if you have to leave the room.

NEVER allow your device to remember your password especially for sensitive data eg when using Google Workspace / Engage or if you are an administrator of any service.

ALWAYS make sure that you cannot be seen entering passwords when in a public place.

THINK whether you really need to be accessing sensitive data over insecure connections eg coffee shops / airports etc

If you have access to Google Workspace / Engage etc via a desktop computer, tablet , laptop, smartphone or any other device MAKE SURE that the device itself has security enabled. This means that to use the device you have to enter a password, swipe pattern, fingerprint or facial recognition etc Consider using a 2-step verification service eg when accessing your Google account you may typically be asked to confirm you are the user by confirming via your mobile phone.

If you lose or have a device stolen and you use it for Google Workspace or Engage YOU MUST INFORM the administrator or school office, they will ensure that your accounts are blocked and passwords are reset.

Other issues

Each user of the school network has the responsibility to have appropriate backgrounds to their desktops. Backgrounds that show violent, abusive, sexual or any other images that would be seen as inappropriate in a school setting, would not be accepted. Profile images / avatars should also follow the same guidelines.

School printers are monitored in a number of ways to maximise efficiency. This may include details of user logins, locations, pages printed, use of colour and double-sided printing. There may be a limit placed on user's accounts. This may take the form of a number of pages during a period of time, limiting colour printing etc. These limits may vary depending on a user's role within school – pupil, staff, manager, administration etc

Some students may need to use ICT resources outside of lesson times. No student is allowed to use ICT resources without supervision. This includes no use of the ICT rooms in break times, before school, after school or during lunchtime without a member of staff present for the whole session. Any student using ICT resources at these times should be actively engaged in material directly linked to coursework set by a member of staff. Not following these rules could result in disciplinary measures.

AIS provides each student and all members of staff who need one with a Google account with the suffix @almunecarinternationalschool.com

These addresses are administered within school and allow full internet access to staff but restricted access for pupils. Changes to this can be made in consultation with the Google school administrator by teachers.

Each of these addresses has access to a large cloud based storage system. Therefore the use of storage facilities like USB sticks, mobile phones or other memory devices is prohibited.

In addition to the email address, this system enables staff and students to communicate electronically and work collaboratively using Google online software known as Google Workspace.

8

The Google email facility should be used sensibly and respectfully, it is expected that students will communicate with members of their own year group mainly. Access to Google email is limited to those who have parental permission to do so and are in Year 4 - 13.

One of the major reasons AIS has developed this system is to protect students and staff from problems otherwise associated with personal email and cloud based storage accounts. As a result, no student should be using any other email address or cloud based storage account within school.

The Google system allows use of email without age restrictions as administrators can restrict use of Google's social media elements within the domain.

BE -

Safe   Responsible   Ethical