

ICT and E Safety Policy

Policy Owner: The British School of Almeria

Policy Area: Safeguarding

Reviewed: July 2025

Next Review: July 2026

RATIONALE AND GUIDANCE

THE BRITISH SCHOOL OF ALMERIA expects that all staff and volunteers in our school and any contractors or partner agency staff used by the school, recognise where a student is at risk of, or is actually being harmed and do all they can to reduce further risk or harm.

The school recognises that ICT and E-safety is an essential element of safeguarding children and adults in the digital world. The internet and Information Communication Technologies are now an important part of everyday life. This document highlights the different areas of ICT and E-safety and the procedures that all members of staff and students within the school are expected to follow.

DEFINITION

The term ICT includes, but is not limited to:

- Any computer, tablet or laptop
- Any device that has access, whether fixed or mobile, to chatrooms, social media, podcasts, instant message services, location tracking technologies and/or GPS.
- Wireless and broadband devices and access
- Mobile phones
- Consoles and gaming devices
- The downloading and broadcasting of music
- Digital cameras
- Display devices such as whiteboards
- Printers or Photocopiers
- Software used for business or education purposes

DIGITAL IMAGES AND VIDEO

The use of video and digital images plays an important part in learning activities. Students and members of staff may use a range of devices to record evidence of activities in lessons and out of school. These images may then be used for a range of educational purposes. It is also recognised that the increased use of technology has increased the potential for devices and images to be misused. To ensure the safety of all students within the school the following guidelines must be adhered to at all times:

1. Photos and Videos of students should be taken on a school camera. Personal devices should only be used as a last resort when no school camera is available.
2. Pictures/videos of any child in the school may only be taken for academic reasons, to be used within the school only (Assessments, displays etc.)
3. Any pictures/videos taken on a personal device of any school child during the school day, whether inside or outside the school building for academic reasons (including trips) **MUST** be downloaded as soon as possible to the School Photos Folder and the pictures/videos immediately removed from the personal device.
4. No pictures/video taken by a member of staff of any child during the school day is allowed to be shared on a personal Social Media account (Twitter, Facebook, Instagram etc.) without prior **written** approval from the principal and/or parents.
5. Any photos/videos of any school children shared between members of staff for academic reasons **MUST** either be downloaded to the official School Photos folder OR must immediately be removed from both devices after being received.
6. No pictures/videos of any school children taken on a personal device during the school day are allowed to be shared with non-members of staff (sent to friends or family using messenger or Whatsapp for example) without prior **written** approval from the Headteacher and/or parents.
7. When prior **written** approval for above mentioned guidelines has been granted by the Headteacher and/or parents, the face of the child/children must be covered/blurred and NO personal details of the child/children are allowed to be shared (name, age etc.)
8. The above guidelines also apply to members of staff who are also parents. Teachers are expected to be professional during the school day. A member of staff is thus expected to request prior approval from the principal before taking pictures of their child(ren) during the school day and/or for special school events when other parents are not at school.

NOTE: When prior **written** approval for above mentioned has been granted by the principal, guideline 7 should be followed.

WEBSITE AND SOCIAL MEDIA

The school will obtain written consent from the parents or guardians at the beginning of the academic year before publishing an image of them or their child(ren) on the school website or social media accounts.

SOCIAL MEDIA

BSA ICT and E Safety Policy

Teachers, students and parents engage with social media applications. These applications include, but are not limited to, Facebook, Snapchat, Instagram,

Twitter, Blogs, and other online tools through which people connect and share information. All members of the school community are expected to uphold the values of the school in all Social Media interactions. Staff, students and parents will not act in such a way that the image of the school is brought into disrepute nor in a way that harms members of the school community.

Guidelines for staff and teacher

1. Social Media in relation to staff and teachers relates to blogs, wikis, podcasts, digital images and video, instant messaging, and mobile devices.
2. Social networking sites such as Facebook or Instagram must not be used by staff as a platform for learning activities with students.
3. Staff should not accept students as 'friends' on their own social network sites or interact with students on social networking sites.
4. Staff and student online interaction must occur only in an educational context.
5. Staff members are advised to NOT accept ex-students or parents of current students as friends on personal Social Media sites.
6. Staff must not discuss students or colleagues or publicly criticise school policies or personnel on social networking sites.
7. Staff should avoid posting comments on social media which could be considered as offensive or disrespectful to an individual or organisation, especially in open forums.
8. Staff members do not have permission to post photos or details that would identify any child on their social media.
9. Staff members are personally responsible for content they publish online. Staff members need to be mindful that what they publish will be public for a long time.
10. Staff must not participate in spreading false or unsubstantiated rumours or false information in regards to the school community and its members.
11. When contributing online, staff should not post confidential student information.
12. Staff should visit their profile security and privacy settings on social networking sites. At a minimum, staff should have all privacy settings set to 'private' and 'only friends'.

E-SAFETY AND ONLINE SAFEGUARDING

The Internet is now an invaluable resource for learning for all our students, and as a school we use it across the curriculum for researching information and as a source for digital learning materials. The internet can however be unsafe when proper procedures are not in place and followed. The following principles should be adhered to in order to ensure the online safety of all students and staff:

1. School Staff
 - o All members of staff are responsible for promoting and supporting safe behaviours in school and following school e-Safety procedures.



BSA ICT and E Safety Policy

- All members of staff must foster a 'No Blame' culture so pupils feel able to report any online bullying, abuse or coming into contact with inappropriate

materials.

- Class teachers should ensure that students are aware of e-Safety rules, introducing them at the beginning of each new school year.
- Class teachers should carefully plan all Internet-based teaching to ensure that pupils are not accidentally introduced to inappropriate content.
- Members of staff will be expected to sign the **Staff Acceptable Internet Use Agreement** annually.

2. Students

- Should be taught to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should be taught the importance of adopting good online safety practice when using digital technologies in and out of school.
- Should be taught to have a good understanding of research skills and the need to avoid dangerous/harmful sites, plagiarism and uphold copyright regulations.
- **Should be taught how to use search engines and how to evaluate Internet-based information as part of the Computing curriculum, and in other curriculum areas where necessary. · Should be taught how to recognise the difference between commercial and non-commercial web sites.**
- Should be taught how to carry out simple checks for bias and misinformation.
- All students are responsible for using the school ICT systems in accordance with **the Student Acceptable Use Policy**, which they will be expected to adhere/agree before being given access to school systems.

3. Parents/Guardians

Parents/guardians play a crucial role in ensuring that their children understand the need to use the Internet / mobile devices in an appropriate way. Many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' information, evenings, supported by the national police; newsletters; emails, the school website and information about national / local online safety campaigns / literature.

Parents and carers will be responsible for:

- Endorsing and accepting the Student Acceptable Use Policy
- Teaching their child(ren) the importance of adopting good online safety practice when using digital technologies in and out of school.

4. Portable storage media

Members of Staff are allowed to use portable media storage devices (USB and External Hard Drives) for academic purposes only. If use of such a device results in an anti-virus message, the device should be removed immediately, and a report must be sent to the School Computing Administrator/ IT-Technician. Staff and students should avoid using any USB device if they are not previously aware of the source and/or content stored.

BSA ICT and E Safety Policy

5. Downloading files and applications

The Internet is a rich source of free files, applications, software, games, and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of school equipment.

- Members of staff should ensure that they check the reliability of the website and content before downloading material onto a school computer.
- Pupils are NOT allowed to download any material from the Internet unless directed to do so by an appropriate staff member.

6. Content filter

The school uses a sophisticated content filter to ensure that as far as possible, only appropriate content from the Internet finds its way into school. Whilst this filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter.

- All pupils and staff should follow the reporting-guidelines outlined below if this happens, and parents/guardians should be informed where necessary.
- Pupils or staff who deliberately try and access unsuitable materials will be dealt with according as set out in the procedures outlined below.

*Automatic alerts will be sent to the Headteacher if pupils or staff try to access inappropriate materials on a school device

7. Smoothwall

The school uses a system called Smoothwall which detects any irresponsible or concerning comments/behaviour from pupils and staff when accessing the school network. In the event of a concern, a notification is automatically sent to the Headteacher/DSL. These concerns will be followed up by the Headteacher/DSL or a member of the safeguarding team.

8. Online bullying

Online bullying refers to **"the repeated use of electronic communication in any form, on any platform, which would cause harm or distress to another person."**

The school has a Zero-Tolerance approach to bullying and takes any incident of online bullying extremely seriously. Any online bullying will be dealt with by the school following the procedures outlined below.

REPORTING ICT OR E-SAFETY INCIDENTS

1. Any safeguarding concern or misuse of any ICT inside or outside the school should be reported using the school's normal Cause for Concern process "MyConcern" . A report should be sent to the **Designated Safeguarding Lead**. Alternatively, if it was felt that a conflict of interest could occur, then the member of staff should report the incident to any other member of the Safeguarding Team.

BSA ICT and E Safety Policy

If it is suspected that at any stage a child or young person may have been or is considered to be subject to abuse, the school is required to follow the safeguarding policy and safeguarding procedures immediately. No attempt should be made to download, print or send any inappropriate materials found as further offences could be committed by doing so.

2. Staff are able to confiscate mobile phones as a sanction according to the school's internal regulations and directives from the regional Andalusian government. However, staff cannot search a mobile device without the consent of the student's parents. This remains the case, even if they suspect that the phone contains an illegal image. If a family refuses to the contents of an offensive message, image or publication, then the issue must be reported to the DSL and/or the Headteacher who can involve the police, who are able to use their extended search powers.
3. Any allegation about the misuse of ICT will be dealt with in a prompt, fair and sensitive manner. The key priority must be to ensure the safety and well-being of children and young people at all times. The school will deal with any incidents on an individual case by case basis. The school will take into account:
 - The context
 - The intention
 - The impact of the incident
4. The following incidents will always be reported to the Police and/or Children's Social Care: Discovery of indecent images of children and young people.
 - Behaviour considered to be grooming.
 - Sending of obscene materials.
5. If the incident relates to an inadvertent access to an inappropriate website.
 - A written report must be sent to the school IT Technician and the website details will be added to the filtered list.
 - A Safeguarding concern must be logged and shared with the DSL for further investigation.
 - It is important that staff report any inadvertent breaches of the policy to avoid a non-reported event being escalated.
6. If an allegation of misuse is made against a child or young person, then the parents or guardians will be informed and will be advised of the actions the school will take.

Policy created by: Gillian Greaves

Reviewed by: Gillian Greaves

Date: July 2025

To be Reviewed: July 2026