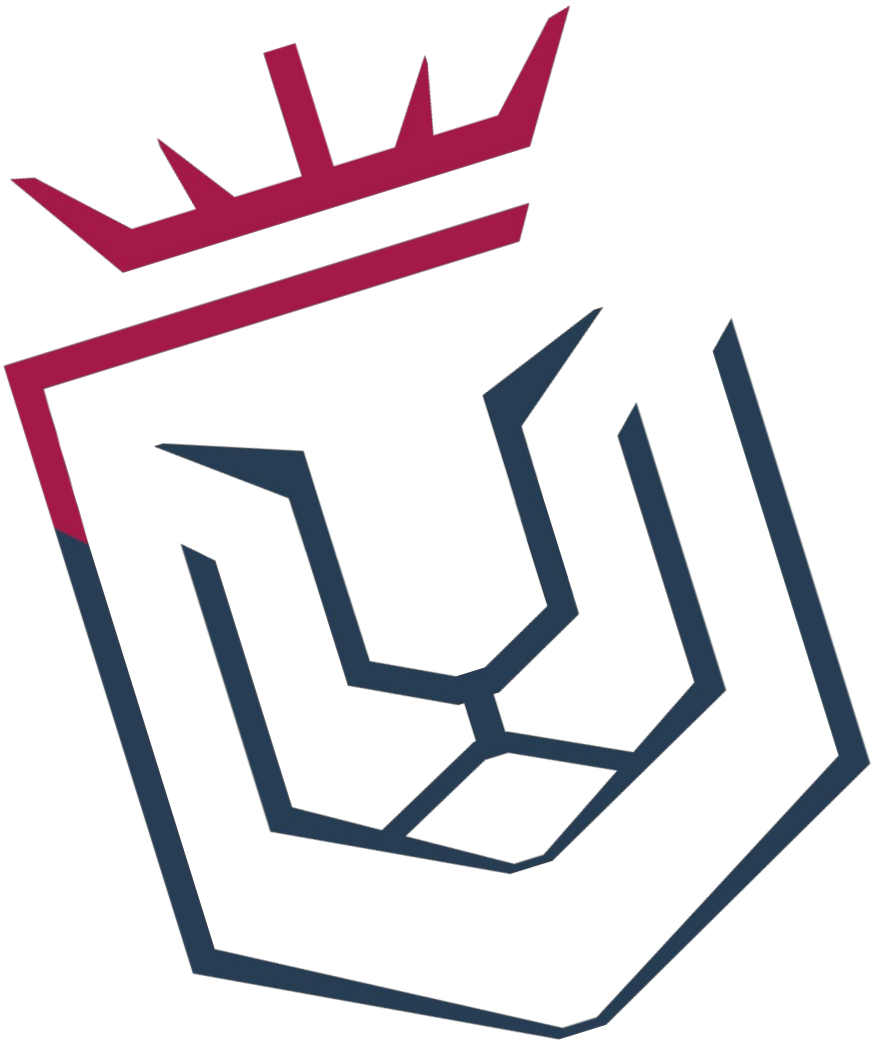
IPS Cascais
BRITISH INTERNATIONAL SCHOOL
PORTUGAL

Safeguarding:

ICT Acceptable Use

Approved Policies for Adoption by Schools



This policy is in conjunction with the School Safeguarding Policy and the Code of Conduct for Staff.

Summary of key policy details

This policy covers, but is not limited to, all devices listed below (private and school-owned):

- School computers
- Mobile telephones
- Digital Tablets
- Mobile games consoles
- Digital cameras
- Digital recording devices
- Smart watches

This policy applies to online behaviour towards other members of the school community inside and outside of school by students or staff, connecting via the Local Area Network (LAN), Wi-Fi networks, mobile data or other means.

User responsibility

Whilst the school embraces the use of technology for educational purposes it also recognises its daily use in social environments and the need to protect students and safeguard the learning environment.

Use of all digital devices should be in line with the school's code of conduct and behaviour expectations. Devices may be used for educational reasons in lessons with the class teacher's permission. Access to the internet must be via school Wi-Fi. 'Hot spotting' is not allowed. It is forbidden to use the school network to access, create or send material, which is offensive in the normal context of a school, or in breach of the law.

Mobile devices should be turned off or set to silent and may not be used when moving around the school campus. Mobile devices must never be used in changing rooms or toilets, when moving about the school campus, at the front of school, in corridors, or the dining room, regardless of the time of day / day of the week.

It is forbidden to distribute information about a member of the school community without their permission, or share any information that defames, undermines, misrepresents, or tarnishes the reputation of the school or its users.

Electronic communication between staff and students must be through official school-approved platforms.

Students and staff should report any suspicious online sexual advances or threatening behaviour to the Designated Safeguarding Lead (DSL) or Head of School, and also to local authorities where appropriate.

The school may, at any time and without further notice, monitor the use of IT systems and online behaviour to maintain safety and also compliance with this policy. It is not permitted to share passwords or log on details for accessing the school network.

The school accepts no responsibility for the safety or replacement of personal devices which are lost, stolen or damaged, unless the device has been issued as part of the school's own digital technology roll-out provision. It is recommended that individuals take out their own insurance for all personal devices.

Behaviour expectations

What individuals do or say online is covered by a number of laws, and increasingly people are being prosecuted for offensive and illegal comments made by electronic communications and on social media sites.

It is at all times forbidden and potentially illegal to use any online or electronic method to send or publish offensive or untrue messages or post unpleasant comments/imagery that could intimidate, harm, or humiliate others. This includes sending or publishing AI created images of others, including deepfake images. To this effect it is strictly against school policy to use a digital device to video, photograph, upload, distribute, store or create material containing another member of the school community without their express permission or that of a member of staff.

Individuals should at no time use digital devices to bully, harass, denigrate, post or distribute private information about a third party whether that be through the use of email, messaging, telephone calls, apps, photographs or video images, social networking or any form of electronic or printed communication. This includes using AI created images of others, including deepfake images.

It is forbidden to use the school network to access, create or send material, which is:

- violent or which glorifies violence
- criminal, terrorist or which glorifies criminal activity (including drug abuse)
- racist or designed to incite racial hatred
- of extreme political opinion, blasphemous or mocking of religious beliefs / values
- racist or homophobic
- could be construed as bullying or harassment
- vulgar, pornographic or with otherwise unsuitable sexual content
- crude or with unsuitable language
- Aims to create a malicious deepfake or AI representation of another member of the community
- offensive in the normal context of a school
- in breach of the law including copyright law, data protection and computer misuse

Any individual who breaches this policy and causes harm or distress to another member of the school community will result in disciplinary action in accordance with school policies.

Any individual caught using a mobile device to cheat in examinations or other formal testing opportunities will face disciplinary actions in line with those as laid down by the relevant

examining body and in line with the school rules.

Protecting identities online

Identity theft is an online danger that is increasing. Students and staff are recommended not to upload or reveal personal details of themselves, their family or other school users online (e.g., address, phone number, date of birth, financial details, passwords etc.) School members should be aware that the use of a mobile device may reveal their precise GPS location at a given date and time, and therefore may reveal movements and locations to third parties.

Unauthorised access to IT systems, accessing others' social networking accounts, e-mail accounts etc., without their permission is an offence. Using generative AI or deepfake technology to create images of others is against company policy.

Reporting concerns

Students should immediately report any suspicious or inappropriate sexual advances, messages or similar online behaviour to their parent, teacher or DSL; they may also report serious or urgent suspicions to the police. Staff should report any concerns to a member of the Leadership Team and safeguarding concerns to the DSL.

Log-ons

By logging onto the school network and any other school IT systems, staff and students agree to the guidelines and policies for ICT use at the school. Passwords should be difficult to guess, and should not be seen by others. It is good practice to have different passwords for different systems rather than the same password for all. IT support must be informed if any member of the school community believes someone has obtained their passwords.

Do not log on to a computing device or any ICT system using another person's password, or use such devices or systems that have been left logged on prior to your use. At the end of a session, all members of the school community should exit and close any IT systems and always log off computers and any password protected sites.

Consequences of Unacceptable Use

The school will act strongly against anyone whose use of ICT could bring the school into disrepute or risks the work of other users; this remains valid even if the incident occurs outside of school. The consequences of misuse, abuse, illegal use or the breaking of any of the rules, as set out in this policy will be dealt with by the Head of School and could include referral to outside agencies such as the Police as appropriate.

Any device that is suspected to have been used to bully, harass or transmit offensive material may be searched by a member of staff, in accordance with the school's search policy.

Students who infringe any of the expectations set out within this policy could face having the devices in question confiscated and permissions to access the school network revoked. Any student device that is used inappropriately in school is liable to be confiscated. Staff must

record any confiscations.

Repeated infringements or refusal, by a student to hand over the mobile device when asked to by a member of staff will be seen as a serious infringement of the school's policies. Should the infringement pertain to a Child Protection matter, the device will be given to the DSL, who will log receipt of the device and act in accordance with the relevant school policy and advice from external agencies.

Theft or damage

All devices should make use of security features to ensure that they cannot be accessed by a third party should they become lost; thereby eliminating the ability of a third party to distribute unsolicited information by pretending to be the owner of the device.

Students and staff are solely responsible for the safekeeping of their devices and should ensure that they are kept securely and marked with the owner's name so they can be returned to their owner if found.

Items that are found and are not clearly marked or identifiable will be handed to the Head of School. Students and staff will be made aware that such devices are held in lost property.

Email

School email addresses are supplied to staff and students for all school-related communication. The school cannot accept responsibility in any way for the content of emails transmitted or received by third-party email servers.

Monitoring & Filtering

The welfare of students is of paramount importance. To this end, the school uses systems to monitor internet use and e-mail traffic whilst respecting privacy at all times. The school reserves the right to inspect data files and network logs if automatic detection of illicit content is triggered.

Manual investigation of email transmissions will only be carried out with the approval of the Head of School or another member of the Senior Leadership Team. Emails may be automatically forwarded to IT Support when detecting viruses, forbidden words, forbidden attachment file types.

Although the school cannot control the content of the Internet, third-party software is used to block sites which are illegal. Filters are constantly updated and amended to prevent unacceptable media entering the school system. Parents are encouraged to contact the IT staff if they have any concerns over the use of email or the internet by their child.

Liability

The school accepts no responsibility for the repair or replacement of personal mobile devices

that are lost, stolen or damaged whilst on school property or during extracurricular activities, trips or when travelling to and from school on school transport. It is recommended that staff/parents/guardians take out their own insurance for all personal devices not issued by the school.

Although the systems offer a very high level of protection, the school cannot be held responsible or accept liability for any damage or loss of data, or the consequences of such damage or loss, whilst any member of the school uses the school system. The school accepts no liability for any damage caused by any type of computer virus, however it originates. The school accepts no liability in the unlikely event that damage is sustained to a privately owned computer as a result of its being connected to the network.
The school accepts no liability for any damage caused if AI is used to deceive or impersonate.

Any questions regarding this policy should be directed to the Head of School.