Version:	Final
Approved:	Sept 2026
Review:	November 2027

The British School of Gran Canaria
Staff Digital Expectations Policy

Contents

1. Rationale
2. Scope
3. Principles
4. Professional Digital Conduct
5. Safeguarding and Online Safety
6. Student Communication
7. Personal Devices
8. School Devices
9. Filtering and Monitoring
10. Classroom Digital Practice
11. Student School Devices
12. Sixth Form Personal Devices
13. Passwords and Account Security
14. Data Protection and Confidentiality
15. Email and Digital Communication
16. Social Media
17. Artificial Intelligence
18. Online Teaching and Meetings
19. Cybersecurity
20. Use of Removable Media
21. Artificial or Altered Images and Recordings
22. Accessibility and Inclusion
23. Reporting Concerns
24. Monitoring and Assurance
25. Staff Training
26. Breaches of the Policy
27. Staff Declaration

1. Rationale

The British School of Gran Canaria recognises that digital technology is an essential part of modern education and provides significant opportunities to enhance teaching, learning, communication and student development.

However, technology also presents risks to students, staff and the school. These include inappropriate online content, cyberbullying, inappropriate communication, data breaches, misuse of artificial intelligence, excessive screen use, cyberattacks and attempts to circumvent school safeguarding and security systems.

The purpose of this policy is to establish clear expectations for all staff so that digital technology is used:

- safely;
- professionally;
- responsibly;
- ethically;
- appropriately;
- in support of high-quality teaching and learning; and
- in a manner that safeguards students and staff.

The school expects all staff to understand that online safeguarding is part of safeguarding and that responsibility for protecting students from online harm rests with everyone.

The policy should be read alongside BSGC's safeguarding, data-protection, employment and other relevant policies and procedures.

2. Scope

This policy applies to all employees and adults working on behalf of BSGC, including:

- teaching staff;
- administrative and support staff;
- supply and temporary staff;
- volunteers;
- Governors when acting on behalf of the school;
- contractors and other adults provided with access to school systems.

The expectations apply whenever staff:

- use school devices;
- access school systems;
- use the school network;
- communicate with students or families electronically;
- teach or supervise students online; or
- use personal devices in connection with their professional role.

Where a contractor or third party has access to BSGC systems, the school may require compliance with equivalent digital-security and safeguarding requirements through the relevant contractual arrangements.

3. Principles

BSGC's approach to digital technology is based on the following principles:

Safeguarding - Digital technology must support, and never undermine, the safety and wellbeing of students.
Professionalism - Staff are expected to maintain professional standards online equivalent to those expected in person.
Proportionality - Digital controls and monitoring will be appropriate to the legitimate safeguarding, security, educational and operational purposes for which they are implemented.
Privacy - The school recognises staff members' rights to privacy and will not seek to monitor or access personal information unnecessarily.
Accountability - Staff remain personally responsible for their professional digital conduct and for reporting concerns.
Security - Staff must protect school information, systems, devices and accounts from unauthorised access.
Continuous improvement - Digital risks evolve rapidly and the school will regularly review its controls, procedures and training.

4. Professional Digital Conduct

Staff are expected to maintain the same high standards of professional conduct online as they would in person.
Staff must:

- use appropriate and professional language;
- maintain appropriate professional boundaries;
- consider how online activity may be perceived by students, parents, colleagues and the wider community;
- protect the reputation of BSGC;
- avoid online activity that could reasonably undermine confidence in their professional role;
- follow the Staff Code of Conduct when using digital technology.

Staff should assume that digital communication may be retained, forwarded, copied or made public, even where they believe it to be private.

Nothing in this policy is intended to regulate lawful private activity unnecessarily. However, staff should recognise that public online activity may have professional consequences where it affects professional boundaries, safeguarding, confidentiality or the reputation of the school. Staff must also be aware that there are clear and stringent laws that control and guide practice and behaviour in this area, and the school community to bound by these regulations.

5. Safeguarding and Online Safety

Safeguarding is everyone's responsibility.

Staff must remain alert to online safeguarding concerns, including:

- cyberbullying;
- online sexual abuse or exploitation;
- inappropriate sexualised communication;
- harmful or extremist material;
- self-harm or suicide-related content;
- online radicalisation;
- grooming;
- inappropriate use of social media;
- image-sharing;

- online harassment;
- threats or intimidation;
- harmful AI-generated or manipulated content.

Any concern relating to a student's online safety must be reported immediately through the school's safeguarding procedures.

Staff must not investigate safeguarding concerns themselves or attempt to determine whether a concern is genuine before reporting it.

Staff must never promise a student that information shared with them will remain confidential.

The school's safeguarding arrangements, including the relevant BSGC safeguarding protocols and the responsibilities of the Designated Safeguarding Lead and Wellbeing and Protection Coordinator, must be followed.

BSGC will provide appropriate training so that staff understand their responsibilities in relation to digital safety and the prevention, identification and reporting of online harm. This reflects the Spanish legal framework requiring educational establishments to have appropriate safeguarding arrangements and digital-safety training.

6. Student Communication

Staff must maintain appropriate professional boundaries when communicating with students. School-approved platforms and communication systems must be used for professional communication.

Staff must not:

- communicate with students through personal social-media accounts;
- use personal messaging applications for routine student communication;
- exchange personal telephone numbers with students unless specifically authorised;
- communicate with students through private or disappearing-message services;
- communicate with students using personal email accounts;
- create private online groups with students unless specifically authorised for an educational purpose.

Where electronic communication with students is required, staff should use school-approved platforms and, where appropriate, ensure that communication is visible to or accessible by other members of staff.

7. Personal Devices

Personal mobile phones, laptops, tablets and other personal devices must not be used in a way that compromises student safeguarding, confidentiality, data protection or professional conduct.

Staff must not use personal devices to:

- photograph or record students;
- store student information;
- download or retain confidential school documents;
- communicate privately with students;
- access or store safeguarding information;

- record meetings or conversations without appropriate authorisation.

Where photography or video recording of students is required for legitimate school purposes, school-approved equipment and procedures must be used.

Personal devices should not be used during lessons or supervision duties except where there is a clear professional or emergency reason.

Personal-device privacy
The school does not routinely monitor the private contents of staff-owned devices.
Where a personal device is used to access BSGC systems, staff remain responsible for complying with school security and data-protection requirements.
The school may apply appropriate technical security controls to access to BSGC systems where necessary to protect students, personal data or school information.

8. School Devices

School devices are provided primarily for professional purposes.
Staff must:

- keep devices secure;
- use strong passwords;
- lock devices when unattended;
- report loss or theft immediately;
- install only authorised software;
- not disable security or safeguarding software;
- not alter firewall, filtering or device-management settings;
- apply security updates when required;
- avoid leaving devices unattended in public areas;
- return equipment when requested.

Staff must not attempt to circumvent school security controls.
This includes attempts to use:

- VPNs;
- proxy services;
- unauthorised browsers;
- alternative DNS services;
- unauthorised applications;
- external storage devices;
- personal hotspots or alternative networks;

where doing so is intended to bypass school security, filtering or safeguarding controls.

9. Filtering and Monitoring

BSGC uses filtering and monitoring systems to protect students, support safeguarding and protect school systems.

Staff should understand that activity undertaken using school-provided digital services, devices and networks may be monitored.

Monitoring may include, where technically necessary and proportionate:

- internet activity;

- access to websites;
- security events;
- device compliance;
- application use;
- network activity;
- attempts to access blocked content;
- cybersecurity events.

Monitoring is undertaken for legitimate purposes including:

- safeguarding;
- cybersecurity;
- protection of school systems;
- compliance with professional responsibilities;
- operational management; and
- maintaining a safe educational environment.

Privacy and proportionality
Monitoring will be conducted in accordance with applicable data-protection law and the school's privacy information.

The school will seek to:

- collect only information necessary for the stated purpose;
- restrict access to monitoring information to authorised personnel;
- retain information only for as long as necessary;
- protect monitoring information from unauthorised access;
- use monitoring information proportionately;
- distinguish between routine monitoring and targeted investigation.

The school will not use monitoring as a means of unrestricted surveillance of staff.

For employees, access to the content of digital devices supplied by the employer is subject to the applicable Spanish legal framework, including the employee's right to privacy and the requirement that access be for legitimate employment-control or device-integrity purposes.

Staff will be informed of the criteria governing the use of school-provided digital devices and systems.

Staff must not attempt to disable, circumvent or interfere with filtering or monitoring systems. Staff should report any apparent weakness in filtering or monitoring to the IT Manager immediately.

10. Classroom Digital Practice

Technology should enhance learning rather than become a distraction.

Teachers should:

- use technology purposefully;
- ensure students understand the learning objective;
- supervise students when using devices;
- actively monitor student activity;
- use available classroom monitoring systems where appropriate;
- ensure students are using approved resources;

- challenge inappropriate use immediately;
- ensure devices are closed or put away when they are not required.

Digital monitoring systems are an additional safeguard and do not replace active classroom supervision. Teachers remain responsible for maintaining appropriate supervision of students.

11. Student School Devices

As BSGC moves away from personally owned devices for Years 7–11, staff have a particular responsibility to model and support responsible use of school-managed devices.
Staff should:

- ensure devices are used only when required;
- remind students that school devices and networks are subject to filtering and monitoring;
- report attempts to circumvent security;
- report inappropriate content or online behaviour;
- follow the school's behaviour procedures where technology is misused;
- liaise with IT and safeguarding staff where concerns arise.

Students must not be permitted to use technology in a way that undermines school filtering, monitoring or safeguarding systems.

12. Key Stage 5 Personal Devices

Year 12 and 13 students may use personal devices in school subject to the KS5 Personal Device Policy and Protocol.

Staff must understand and consistently apply the expectations contained in that protocol.
In particular, staff should:

- ensure personal devices are being used for appropriate educational purposes;
- challenge inappropriate use;
- report attempts to circumvent school filtering or network controls;
- report the use of unauthorised networks, personal hotspots or other methods intended to bypass school controls;
- follow the agreed escalation process.

Where a safeguarding, cybersecurity or serious behavioural concern arises, staff should follow the relevant BSGC procedure and refer the matter to the appropriate member of staff.

13. Passwords and Account Security

Staff must:

- keep passwords confidential;
- never share passwords with students or other staff;
- use strong passwords;
- use multi-factor authentication where provided;
- lock devices when leaving them unattended;
- report suspected compromised accounts immediately;
- never use another person's account.

Passwords must not be written where they can be easily accessed by others.
Staff should remain alert to phishing and social-engineering attempts.

14. Data Protection and Confidentiality

Staff have a professional and legal responsibility to protect personal and confidential information. This includes information relating to:

- students;
- families;
- staff;
- safeguarding;
- medical needs;
- educational records;
- assessments;
- personnel matters.

Staff must:

- only access information required for their role;
- use approved systems to store information;
- check recipients before sending sensitive information;
- avoid sending confidential information through personal email;
- avoid storing school information on personal devices;
- use secure methods when transferring sensitive information;
- report suspected data breaches immediately.

The school will apply the principles of data minimisation, purpose limitation, confidentiality, security and appropriate retention to digital information.

The use of digital platforms and applications must be approved in accordance with BSGC's data-protection arrangements. Particular care must be taken where platforms process children's data or transfer data to third parties. The AEPD (*Agencia Española de Protección de Datos*) has specifically highlighted these risks in its current guidance for educational establishments.

Data-protection requirements must never be interpreted as preventing necessary safeguarding information from being shared with the appropriate person.

15. Email and Digital Communication

Staff emails should be:

- professional;
- accurate;
- proportionate;
- respectful;
- appropriate for potential future disclosure.

Staff should take particular care when communicating about:

- student behaviour;
- safeguarding;
- complaints;
- disciplinary matters;
- confidential family circumstances.

Sensitive information should only be shared with those who have a legitimate need to receive it.

16. Social Media

Staff should exercise professional judgement when using social media.
Staff must not:

- post confidential school information;
- identify students without appropriate authorisation;
- publish photographs of students from personal accounts;
- engage in inappropriate online discussions about students or families;
- post material that could reasonably undermine their professional role or the reputation of the school.

Staff should carefully consider whether social-media activity could create a conflict between their personal and professional responsibilities.

The school does not seek to regulate lawful private activity unnecessarily. However, staff should recognise that public online activity may have professional consequences.

17. Artificial Intelligence

BSGC recognises that generative AI is an important and rapidly developing educational technology. Staff are expected to use AI responsibly, ethically and professionally.

AI may be used to support appropriate activities such as:

- lesson planning;
- generating ideas;
- creating resources;
- differentiation;
- administrative tasks;
- drafting non-confidential communications;
- professional development.

Staff must not enter confidential or personally identifiable student, parent or staff information into public AI tools unless the platform has been specifically approved by the school for that purpose.
AI-generated material must be checked for:

- accuracy;
- bias;
- appropriateness;
- copyright concerns;
- factual errors;
- suitability for students.

Staff remain professionally responsible for material produced with AI assistance.
AI must not replace professional judgement.

18. Online Teaching and Meetings

Where staff teach or meet students online, they must use school-approved platforms and follow safeguarding procedures.
Staff should:

- use professional accounts;
- use appropriate backgrounds and locations;
- ensure that other people cannot inadvertently be heard or seen;

- maintain appropriate dress and professional conduct;
- avoid private one-to-one communication unless necessary and authorised;
- follow school procedures for recording online sessions.

Any recording must have a legitimate educational or safeguarding purpose and be handled in accordance with school policy and data-protection requirements.

19. Cybersecurity

All staff are part of BSGC's cybersecurity protection.
Staff must:

- complete required cybersecurity training;
- remain alert to phishing;
- not open suspicious attachments or links;
- verify unusual requests for information or payments;
- report suspected cyber incidents immediately;
- protect school devices from unauthorised access.

Examples of incidents that must be reported include:

- suspected phishing;
- lost or stolen devices;
- accidental disclosure of information;
- compromised passwords;
- malware;
- suspicious emails;
- unauthorised access;
- attempts to circumvent security systems.

Staff should report concerns to the IT Manager and, where relevant, the DSL or Director of Operations.

20. Use of Removable Media

USB drives and other removable storage should only be used where authorised.

Staff should not use unknown or personal USB devices to transfer school information.

Sensitive information must not be transferred to removable media unless specifically authorised and appropriately secured.

21. Artificial or Altered Images and Recordings

Staff must exercise particular caution regarding photographs, videos, deepfakes and AI-generated or manipulated content involving students.

Staff must report concerns where students appear to be:

- creating inappropriate images;
- manipulating images of other students;
- sharing sexualised images;
- using AI to impersonate others;
- creating threatening or humiliating material.

Such activity may constitute a safeguarding or behaviour concern and must be dealt with through the appropriate school procedures.

22. Accessibility and Inclusion

Digital technology should support equitable access to learning.
Staff should consider the needs of students who require:

- assistive technology;
- accessibility features;
- alternative formats;
- additional digital support.

The school expects staff to use available accessibility tools appropriately and to seek support where a student's digital access needs are not being met.

23. Reporting Concerns

Staff should report:

Concern	Report to
Safeguarding	DSL or Deputy DSL
Technical or cybersecurity	IT Manager
Data protection	Designated Data Protection Lead
Behavioural misuse	Relevant Head of School / Head of Key Stage
Serious or repeated concerns	Head / Director of Operations / DSL as appropriate

Staff must not delay reporting because they are uncertain whether an incident is sufficiently serious. If in doubt, report it.

Where a concern may involve an immediate risk to a child, staff must follow the school's safeguarding procedures without delay.

24. Monitoring and Assurance

The school will monitor compliance with this policy through appropriate and proportionate measures including:

- IT security reports;
- filtering and monitoring reports;
- device-management reports;
- safeguarding records;
- behaviour records;
- staff training records;
- incident reporting;
- periodic policy review;
- audits of digital systems;
- staff and student feedback.

The Director of Operations and IT Manager will maintain oversight of technical controls.
The DSL will maintain oversight of online safeguarding concerns within their respective responsibilities.

The Data Protection Lead will advise on data-protection implications and compliance.
The Head retains overall responsibility for ensuring that the school has appropriate arrangements in place.
The school's governing body will receive appropriate assurance regarding digital safeguarding, cybersecurity and significant digital risks.

25. Staff Training

All staff will receive appropriate training on:

- online safeguarding;
- acceptable digital use;
- cybersecurity;
- phishing and social engineering;
- data protection;
- AI;
- professional digital communication;
- use of school monitoring systems.

Training will be provided:

- during induction;
- annually;
- following significant changes to systems or policy;
- when emerging risks require additional training.

Training records will be maintained by the school.

26. Breaches of the Policy

Failure to comply with these expectations may result in:

- additional training;
- withdrawal or restriction of access to systems;
- management action;
- disciplinary action;
- referral under safeguarding procedures;
- referral to external authorities where appropriate.

The response will be proportionate to the circumstances and consistent with the school's relevant policies, contractual arrangements and applicable employment procedures.

Any disciplinary action involving an employee will be undertaken in accordance with the applicable employment framework and the employee's rights.

Deliberately attempting to circumvent safeguarding, filtering or cybersecurity controls will be regarded as a serious matter.

Nothing in this policy removes or alters any statutory reporting obligation or the school's safeguarding responsibilities. Any contravention of the law has to be reported to the relevant authorities.

27. Staff Declaration

All staff are required to confirm that they:

1. Have read and understood this policy.
2. Understand that digital safeguarding is part of their safeguarding responsibilities.
3. Will use school technology responsibly and professionally.
4. Will maintain appropriate professional boundaries online.
5. Will protect confidential information.
6. Will not attempt to circumvent school filtering, monitoring or cybersecurity controls.
7. Will report safeguarding, data-protection and cybersecurity concerns promptly.
8. Understand that use of school-provided systems and devices may be monitored for legitimate safeguarding, security and operational purposes.
9. Understand that monitoring will be undertaken in accordance with applicable data-protection requirements and the school's privacy information.
10. Understand that personal devices remain subject to the school's professional and safeguarding expectations when used in connection with their professional role.

Name: _____

Signature: _____

Date: _____