

The British School of Gran Canaria



Digital Safeguarding and Device Management Policy

Policy Owner: Designated Safeguarding Lead (DSL)

Operational Lead: IT Manager

Table of Contents

1. Rationale and Purpose	4
2. Scope.....	4
3. Core Principles	5
4. School-Controlled Devices	5
5. Device Configuration.....	5
6. Student Accounts	6
7. Filtering	6
8. Monitoring	7
9. Classroom Supervision	7
10. Classroom Management Technology	7
11. Circumvention of School Controls	8
12. Mobile Phones	8
13. Personal Devices	8
Students in Years 1–11.....	8
Students in Years 12–13.....	8
14. Unauthorised Software and Applications	9
15. USB Devices and External Storage	9
16. Home Use.....	9
17. Safeguarding Alerts	9
18. Cybersecurity Incidents.....	10
19. Lost or Stolen Devices	10
20. Data Protection	11
21. Privacy and Transparency	11
22. Artificial Intelligence	11
23. Students with Additional Needs	11
24. Staff Responsibilities	12
Teachers	12
IT Manager	12
DSL.....	12
Director of Operations	13
Head / SLT	13
Governing Body.....	13
25. Student Responsibilities.....	13
26. Parents and Carers.....	13
27. Misuse and Consequences.....	14
Low-level misuse.....	14

Serious misuse	14
Very serious/deliberate misuse	14
28. Technical Testing and Assurance	14
29. Automatic Safeguarding Reports	15
30. Annual Review	15
31. Digital Safeguarding Operating Model.....	16
32. Legal and Regulatory Framework	16
33. Child Protection, Wellbeing and Online Violence.....	17
34. Illegal or Seriously Harmful Online Content	17
35. Monitoring, Filtering and Data Protection.....	18
36. Digital Education and Staff Training.....	18
37. Canary Islands Protocols and Local Procedures.....	19
38. Monitoring Data Schedule and Retention	19
39. Online Safety Incident Response	19
40. Legal Compliance Review and Assurance	20
41. Related BSGC Policies and Procedures	20

1. Rationale and Purpose

BSGC recognises that technology is an essential part of contemporary education and provides significant opportunities for learning, communication, creativity and collaboration. At the same time, digital technology creates risks to students' safety, wellbeing, privacy, learning and personal development.

The purpose of this Policy is therefore to ensure that BSGC provides a digital environment in which:

- technology supports high-quality learning;
- students are protected from inappropriate and harmful online content;
- digital activity is appropriately monitored;
- school devices are securely managed;
- students develop responsible digital behaviours;
- personal information is protected;
- staff understand their responsibilities;
- inappropriate or unsafe use is identified and addressed promptly.

The school's approach is based on the principle that digital safeguarding is an integral part of safeguarding, not a separate IT issue.

2. Scope

This Policy applies to:

- all BSGC students;
- all teaching and support staff;
- governors;
- temporary and agency staff;
- volunteers;
- contractors and visitors using school systems;
- parents/carers where they interact with school digital systems.

This Policy's monitoring provisions primarily concern students and school-managed devices. It does not, by itself, authorise monitoring of staff devices or accounts. Any staff monitoring must be governed separately through the Staff Digital Expectations Policy and applicable employment, consultation, transparency and data-protection requirements.

It applies to:

- school-owned laptops and tablets;
- school networks and Wi-Fi;
- school accounts;
- school supplied cloud services;
- educational platforms;
- email;
- internet access;
- online learning;
- classroom-management software;
- filtering and monitoring systems;
- mobile devices where connected to or used within the school environment;
- approved personal devices;
- AI and other emerging technologies.

For students from Early Years Foundation Stage (EYFS) to Year 11, BSGC's principal model is access to school-provided and school-managed devices where required for learning. The school may use shared devices or class sets; this statement does not commit BSGC to a dedicated 1:1 device allocation.

The separate KS5 Personal Device Protocol governs personal laptops brought into school by students in Years 12–13.

3. Core Principles

BSGC's approach is based on eight principles:

1. Learning first - Technology should enhance learning rather than become a distraction from it.
2. Safety by design - Devices and systems should be configured to minimise foreseeable risks before they are provided to students.
3. Appropriate control - Students should have access to the technology and information they need for learning, but not unrestricted access where this creates unnecessary risk.
4. Proportionate monitoring - Digital activity may be monitored where necessary to safeguard students, maintain appropriate use and protect school systems.
5. Privacy and transparency - Monitoring and data processing will be lawful, proportionate and communicated appropriately.
6. Personal responsibility - Students are expected to use technology responsibly and understand that attempts to circumvent school controls are unacceptable.
7. Human supervision - Technology does not replace teachers' professional judgement or active supervision.
8. Education alongside protection - Students should learn how to recognise and manage digital risks rather than simply being protected from them.

4. School-Controlled Devices

BSGC will provide access to school-controlled devices for students from EYFS to Year 11 where required for learning. Devices may be shared or provided as class sets in line with the school's educational needs and resourcing model. These devices will be:

- owned or controlled by the school;
- registered by the school;
- configured by IT;
- connected to school security systems;
- subject to appropriate filtering and monitoring;
- protected by security software;
- updated and patched centrally;
- configured with approved applications;
- subject to appropriate restrictions on installation and configuration.

The purpose is not to reduce students' access to technology but to ensure that technology is safe, consistent, reliable and educationally purposeful.

5. Device Configuration

Before a device is issued to a student, IT will ensure that it has, as appropriate:

- secure operating-system configuration;
- current security updates;
- endpoint protection;
- school-managed user accounts;
- appropriate authentication;
- web filtering;
- monitoring;
- device-management software;
- approved applications;
- appropriate browser configuration;
- secure Wi-Fi configuration;
- restrictions on unauthorised software;
- appropriate storage and synchronisation arrangements.

New devices will be tested for filtering and monitoring before being distributed to students.

6. Student Accounts

Each student should have an identifiable school account. Students must:

- use their own account;
- keep passwords confidential;
- not share accounts;
- not attempt to access another student's account;
- log out where appropriate;
- report compromised credentials.

Shared student accounts will be avoided unless there is a clearly justified operational or practical reason. The ability to identify the user of a device is particularly important where monitoring identifies a safeguarding concern.

7. Filtering

BSGC will maintain appropriate web and content filtering to reduce access to:

- illegal content;
- adult content;
- harmful content;
- inappropriate material;
- malicious websites;
- known security threats;
- inappropriate services or applications.

Filtering will be age-appropriate and risk-based. Filtering will not unnecessarily prevent legitimate educational activity.

The school uses a commercial categorisation system for web sites and applications. The DSL/SLT are responsible for defining the categories that are available to students in different age groups.

The school recognises that no filtering system is perfect. Filtering therefore forms one part of a wider safeguarding system and does not replace supervision, education or monitoring.

8. Monitoring

BSGC will use appropriate technical monitoring of school-managed devices and networks.

Monitoring may identify:

- searches;
- websites accessed;
- attempts to access blocked content;
- inappropriate or harmful activity;
- suspicious activity;
- attempts to circumvent controls;
- malware or security threats;
- potentially serious safeguarding concerns.

Monitoring information will only be accessible to appropriately authorised personnel. Monitoring systems should generate alerts that can be reviewed and acted upon promptly where necessary. Current guidance distinguishes monitoring from filtering: filtering seeks to prevent access, while monitoring identifies and enables intervention in concerning activity.

9. Classroom Supervision

Technical monitoring does not replace teacher supervision. Teachers remain responsible for actively supervising students when they are using devices. Teachers should:

- circulate and observe screens;
- ensure students are using the correct application or website;
- challenge inappropriate use;
- prevent students from using devices for unrelated activity;
- report concerns;
- ensure devices are used appropriately during lessons.

10. Classroom Management Technology

Where appropriate, BSGC may use a classroom management system to allow teachers to remotely:

- view student screens;
- share the teacher's screen;
- restrict access to particular websites;
- direct students to specific resources;
- lock screens;
- close inappropriate applications;
- support focused learning.

Use of such a system must be:

- educationally justified;
- proportionate;
- appropriately configured;
- transparent;
- consistent with the Data Protection Policy.

11. Circumvention of School Controls

Students must not attempt to bypass, disable or undermine BSGC's digital controls. This includes attempting to use:

- VPNs;
- proxy servers;
- alternative DNS services;
- unauthorised browsers;
- personal hotspots;
- mobile tethering;
- USB/network adapters;
- unauthorised operating systems;
- portable applications;
- remote-access software;
- unauthorised cloud services;
- encryption or other tools intended to conceal activity;
- alternative accounts;
- unauthorised extensions;
- other methods designed to circumvent school security or monitoring.

Attempts to circumvent controls will be treated as very serious/deliberate misuse of school technology, even where the student does not ultimately access inappropriate content.

12. Mobile Phones

BSGC operates a phone-free approach during the school day in accordance with the school's mobile-phone arrangements. Where students bring phones to school, they must comply with the school's requirement to hand them in and must not use them to circumvent school network or device controls by using;

- personal hotspots;
- tethering;
- mobile data;
- Bluetooth-based network connectivity;
- other personal-device connections

The use of a personal device to circumvent school safeguards will be treated as very serious/deliberate misuse under Section 27.

13. Personal Devices

Students in Years 1–11

Personal devices are not normally permitted for routine learning.

Students will use school-provided devices when necessary.

Students in Years 12–13

KS5 students may bring personal laptops subject to the separate KS5 Personal Device Protocol.

KS5 students remain subject to:

- school network controls;
- Acceptable Use Policy;
- filtering;

- monitoring of traffic on the school network only; no monitoring software will be installed on a privately owned KS5 device unless expressly provided for in the KS5 Personal Device Protocol, following appropriate privacy and data-protection review;
- safeguarding requirements;
- restrictions on tethering and circumvention.

14. Unauthorised Software and Applications

Students must not:

- install unauthorised software;
- install games;
- install VPN software;
- install or configure proxy tools;
- install software designed to circumvent restrictions;
- disable security software;
- modify device-management settings;
- alter network configurations;
- obtain administrator privileges.

IT may remotely remove unauthorised software or restrict a device where necessary.

15. USB Devices and External Storage

The use of USB drives and other external storage devices may be restricted. Students must not connect:

- unauthorised USB devices;
- unknown storage devices;
- personal network adapters;
- devices intended to circumvent controls.

Where USB storage is permitted for legitimate educational purposes, appropriate malware and security controls should apply.

16. Home Use

Occasionally the school may provide devices to be taken home, the school's security controls should remain active. Students and parents should understand that:

- A school-owned device remains a school-managed device when it is outside school.
- Where technically possible, filtering, device management and security controls should continue to operate off-site. Off-site use must be covered by the relevant privacy information and DPIA where required; routine individual-level browsing monitoring outside school must not take place unless it has a documented lawful basis, is necessary and proportionate, and has been clearly communicated.
- Students remain subject to the school's Acceptable Use Policy when using school supplied devices outside school.

17. Safeguarding Alerts

Where filtering or monitoring identifies potentially harmful or concerning activity, the matter should be assessed promptly. Potential concerns may include:

- self-harm;

- suicidal ideation;
- sexual exploitation;
- AI-generated or digitally manipulated sexual imagery of a child (including deepfakes and “deepnude” images), whether the child depicted is a BSGC student or otherwise;
- grooming;
- abuse;
- bullying;
- extremist content;
- criminal exploitation;
- inappropriate sexual content;
- threats of violence;
- serious emotional distress.

Staff should be aware that AI-generated and digitally manipulated imagery is a recognised and growing safeguarding risk, and that such content must be treated with the same seriousness as other child-on-child abuse or sexual exploitation concerns, regardless of whether the image is “real.”

The DSL remains responsible for safeguarding decisions. IT staff will act in an advisory role to the DSL to help understand the nature of an incident.

18. Cybersecurity Incidents

Students must immediately report:

- suspicious pop-ups;
- malware;
- compromised accounts;
- phishing;
- stolen devices;
- unexpected software;
- security warnings;
- suspected hacking;
- loss of confidential information.

Students must not attempt to investigate or resolve a serious technical security incident themselves.

19. Lost or Stolen Devices

A lost or stolen school device must be reported immediately. The IT Manager will coordinate the response, using device-management tools where appropriate, and will:

- identify the device;
- *use device-location functionality only after the device has been reported lost or stolen, where enabled, lawful and necessary;*
- disable or lock it where possible;
- assess whether information may be accessible;
- determine whether remote-wipe action is required;
- record the incident;
- notify safeguarding staff where appropriate.

20. Data Protection

All digital monitoring and device management must comply with the BSGC Data Protection Policy.

This includes appropriate consideration of:

- lawful basis;
- transparency;
- data minimisation;
- retention;
- access controls;
- security;
- children's data;
- DPIAs (Data Protection Impact Assessment);
- third-party processors.

Before a new monitoring or filtering system is introduced, or existing monitoring is materially changed, BSGC shall determine the lawful basis and complete a Data Protection Impact Assessment (DPIA) where required. The DSL, IT Manager and Data Protection Officer (DPO) must confirm and document whether a completed DPIA covers the current monitoring software. Where a DPIA is legally required but absent, the relevant processing must not commence or continue until the DPIA has been completed and the required approvals obtained. UK guidance, including Keeping Children Safe in Education and the Department for Education's Filtering and Monitoring Standards, may be used as a reference alongside applicable Spanish and EU requirements.

21. Privacy and Transparency

Students and parents will be informed appropriately about:

- what is monitored;
- why it is monitored;
- who can access monitoring information;
- how alerts are handled;
- how long monitoring information is retained;
- how concerns can be raised.

Monitoring should be proportionate and transparent, not covert simply because technology makes covert monitoring possible.

22. Artificial Intelligence

AI use on school devices must comply with the BSGC AI Policy and AI Use and Approval Procedure.

Students must not:

- upload personal information about themselves or others to public AI systems;
- upload confidential school information;
- upload safeguarding information;
- use AI to impersonate another person;
- use AI to bypass school controls;
- use AI in assessments where prohibited.

Approved AI tools must be appropriately configured and reviewed.

23. Students with Additional Needs

Digital safeguarding arrangements should take account of:

- age;
- maturity;
- SEND;
- language needs;
- individual vulnerabilities;
- safeguarding risks.

Where a student requires a particular accessibility tool or technology, the school should consider how this can be provided safely within the managed environment.

24. Staff Responsibilities

Teachers

Teachers must:

- supervise device use;
- reinforce appropriate use;
- report concerns;
- not allow students to circumvent controls;
- use classroom-management tools appropriately;
- follow safeguarding procedures;
- understand their role and responsibilities in relation to filtering and monitoring.

IT Manager

The IT Manager is responsible for:

- device configuration;
- central management of devices;
- filtering;
- monitoring;
- endpoint security;
- patching;
- account management;
- technical reporting;
- device inventory;
- technical incident response;
- testing controls;
- maintaining technical documentation.

Designated Safeguarding Lead (DSL)

The DSL is responsible for:

- safeguarding concerns arising from monitoring;
- reviewing safeguarding alerts;
- coordinating intervention;
- ensuring appropriate recording;
- reporting to SLT/Governors.

Data Protection Officer (DPO)

The DPO shall advise and monitor compliance in relation to:

- lawful basis, transparency and data minimisation;
- DPIA screening, review and advice;
- monitoring-data access, retention and data-subject rights;
- supplier and processor arrangements, security and international transfers;

- data-protection incidents and any required consultation with the supervisory authority.

Director of Operations

The Director of Operations oversees:

- operational implementation;
- resources;
- procurement;
- contractual arrangements;
- policy implementation;
- cross-departmental coordination;
- assurance reporting.

Head / SLT

The Head of school and the SLT provide strategic oversight and ensures that digital safeguarding forms part of the school's wider safeguarding framework.

Governing Body

Governors shall receive a termly digital-safeguarding assurance report, coordinated by the DSL, IT Manager and DPO, covering:

- aggregated alert numbers by category and safeguarding escalations;
- circumvention attempts and significant incidents;
- filtering and monitoring control-test results and identified remedial actions;
- DPIA status, supplier assurance and material data-protection issues;
- progress against agreed actions and the annual policy review.

25. Student Responsibilities

Students must:

- use school technology for legitimate educational purposes;
- protect their account;
- follow teacher instructions;
- respect others online;
- report concerns;
- look after school devices;
- use only approved software;
- respect filtering and monitoring;
- not attempt to circumvent controls.

Students must understand that access to school technology is conditional upon responsible use.

26. Parents and Carers

Parents are expected to:

- support the school's digital expectations;
- reinforce responsible technology use at home;
- report concerns to the school;
- ensure school devices are appropriately cared for;
- support students in understanding online safety.

Parents should understand that the school's managed-device approach is intended to provide an additional layer of protection and does not remove the need for appropriate parental supervision outside school.

27. Misuse and Consequences

Examples of misuse include:

Low-level misuse

- gaming;
- inappropriate browsing;
- using social media;
- unrelated messaging;
- repeatedly ignoring teacher instructions.

Serious misuse

- accessing harmful material;
- cyberbullying;
- sharing inappropriate images;
- deliberately damaging equipment;
- accessing another student's account;
- installing prohibited software.

Very serious/deliberate misuse

- bypassing filtering;
- using VPNs or proxies to circumvent controls;
- disabling monitoring;
- hacking (un-authorised access to systems);
- deliberately introducing malware;
- attempting to obtain administrator access;
- accessing or distributing illegal material;
- using technology to threaten or exploit others.

Consequences will be proportionate and may include:

- warning;
- removal of device access;
- confiscation or restriction;
- parental contact;
- restorative action;
- issue of a reflection time;
- behaviour sanction;
- safeguarding referral;
- disciplinary action;
- referral to external authorities where required.

28. Technical Testing and Assurance

The IT Manager will maintain a programme of testing to ensure that:

- filtering remains active;
- monitoring remains active;
- new devices are correctly configured;

- security software is functioning;
- students cannot readily circumvent controls;
- accounts are correctly assigned;
- inappropriate access attempts are recorded;
- controls work both on-site and, where applicable, off-site.

29. Automatic Safeguarding Reports

The monitoring software installed on school-supplied devices will be configured to route individual-level safeguarding alerts and detailed activity reports to the DSL and authorised Deputy DSLs. SLT will receive aggregated, non-identifying trend information by default. Identifiable information may be shared with other authorised personnel only where there is a specific safeguarding or operational need and access is necessary and documented.

The automatic weekly summary reports will include:

- Login identities of students who triggered a filter or alert
- The device the student used
- The time of the incident(s)
- The filter/policy that the student triggered

Online real-time monitoring will make detailed individual-level information available only to the DSL and authorised Deputy DSLs, with IT access limited to technical administration or investigation on a need-to-know basis:

- A list of all sites a student has accessed and indicate if access was allowed or blocked
- A summary of search terms the students have been using
- A detailed list of search terms for each student
- Videos individual students have accessed
- Sites or applications students have been blocked from accessing
- A student wellbeing report highlighting trends in sites accessed or search terms that might indicate concerning activities

Routine individual-level online and filtering logs will be retained for no longer than 60 days, then securely deleted or anonymised, unless relevant information is escalated into a safeguarding, disciplinary, legal or security incident record. Escalated records will be retained in accordance with the applicable safeguarding or incident-retention schedule.

The school acknowledges that automated monitoring and reporting systems can generate false-positive alerts. The DSL, in conjunction with the IT Manager and authorised Deputy DSLs where appropriate, will assess alerts and record the rationale for safeguarding action or closure. Alerts must not be treated as proof of wrongdoing without appropriate human assessment.

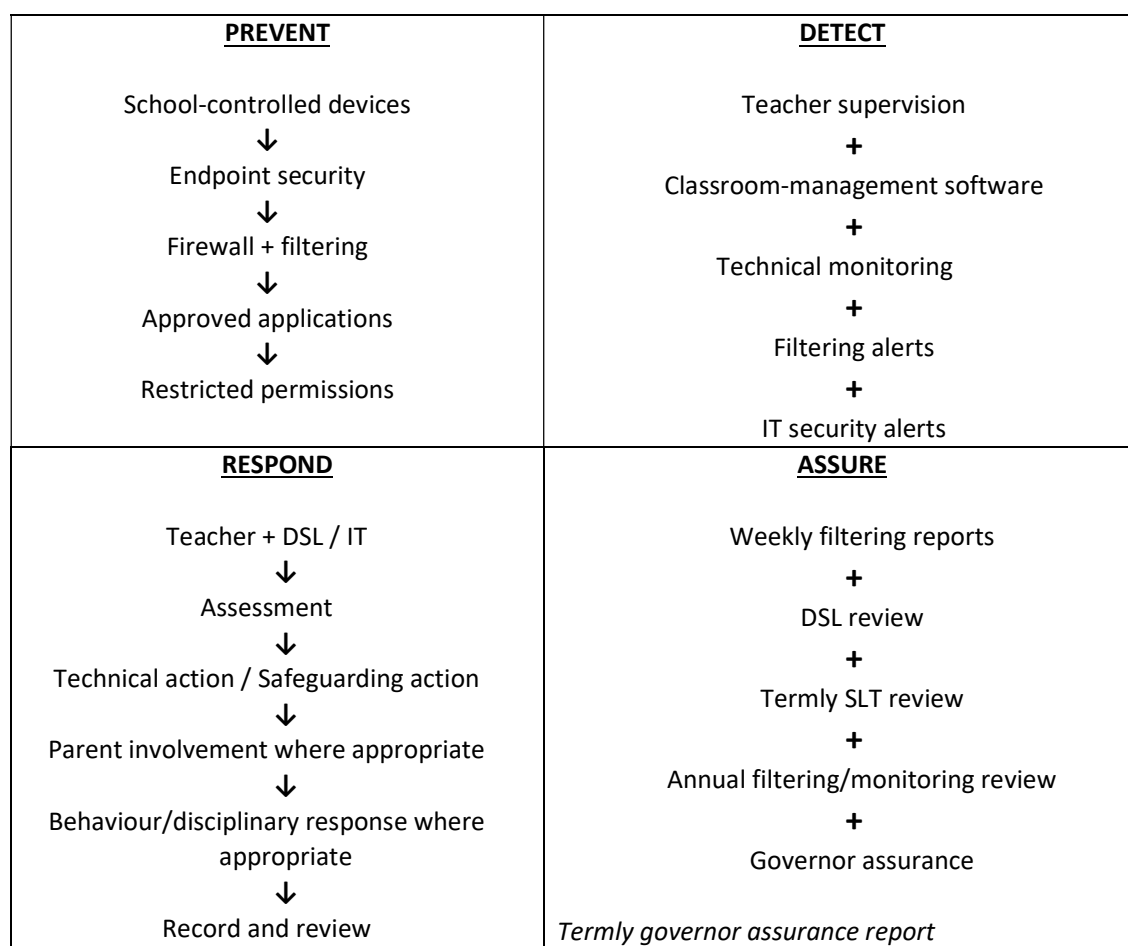
30. Annual Review

BSGC's digital safeguarding and device-management arrangements will be formally reviewed at least annually. In addition, the effectiveness of BSGC's filtering and monitoring systems specifically will be reviewed at least once every academic year, led by the SLT with the support of the DSL and IT Manager. Evidence of this review (including any actions identified and their completion) will be documented and retained. The review shall consider:

- student age and risk profile;
- emerging online risks;

- AI developments;
- filtering effectiveness;
- monitoring effectiveness;
- device security;
- incidents;
- circumvention attempts;
- student and staff feedback;
- safeguarding concerns;
- data-protection requirements;
- supplier performance.

31. Digital Safeguarding Operating Model



32. Legal and Regulatory Framework

This Policy forms part of BSGC's safeguarding, data-protection, behaviour and digital-governance framework. While it is aligned to UK best practices it has been developed in conjunction with the applicable Spanish, European Union and Canary Islands laws. Where a legal requirement conflicts with an operational practice described in this Policy, the legal requirement takes precedence.

- Ley Orgánica 8/2021 (LOPIVI), including Articles 18, 19, 33–35, 45 and 46.

- Ley Orgánica 3/2018 (LOPDGDD), including Articles 82–85 and 92.
- Regulation (EU) 2016/679 (GDPR), including Articles 5, 6, 12–14, 28, 32 and 35.
- Ley Orgánica 2/2006 (LOE), as amended by Ley Orgánica 3/2020 (LOMLOE), including Article 111 bis and applicable digital-competence and online-safety provisions.
- Ley 6/2014, de 25 de julio, Canaria de Educación no Universitaria, including Article 24 concerning virtual educational spaces, digital learning, training, intellectual property and electronic communication.
- Applicable Canary Islands educational, convivencia, safeguarding, anti-bullying, cyberbullying and cybersecurity protocols and instructions.

BSGC shall maintain a current legal and regulatory register for this Policy. The Data Protection Officer (DPO), Designated Safeguarding Lead and Director of Operations shall review material legal changes and ensure that linked policies and procedures are updated. The DPO shall advise on lawful basis, transparency, data minimisation, retention, supplier arrangements and DPIA requirements, and shall be involved in DPIA review and sign-off in accordance with the school's data-protection governance. Before approval and at each annual review, the register shall verify the current status, exact citation and applicability to BSGC of each listed law and local protocol. The proposed Spanish legislation on the protection of minors in digital environments shall be tracked as pending and shall not be treated as enacted unless and until it enters into force.

33. Child Protection, Wellbeing and Online Violence

Digital safeguarding is a component of child protection. Any online activity or technology-enabled conduct that may constitute violence, abuse, exploitation, harassment or serious harm to a student shall be managed through the school's safeguarding framework, not solely as an IT or disciplinary matter.

- BSGC shall maintain a clearly identified Designated Safeguarding Lead (DSL), who is also the Coordinador/a de Bienestar y Protección in accordance with LOPIVI, who will work closely with the SLT and other safeguarding personnel.
- The DSL shall determine the safeguarding response to alerts involving cyberbullying, grooming, sexting, sexual exploitation, online sexual violence, threats, self-harm, suicidal ideation, criminal exploitation or other serious harm.
- IT personnel shall provide technical assistance, preserve relevant evidence securely and implement protective controls, but shall not conduct safeguarding investigations unless specifically authorised under the school's safeguarding procedures.
- Students shall be provided with age-appropriate information about how and to whom they can report online safety concerns.
- Where information indicates violence against a child or potentially unlawful online content, the school shall follow the applicable safeguarding and legal reporting route, including referral to competent authorities where legally required.
- Where notifying parents/carers could increase risk to a child or compromise a safeguarding response, the school shall follow the safeguarding lead's assessment and applicable legal guidance before notification.

34. Illegal or Seriously Harmful Online Content

Where staff or monitoring systems identify material that may constitute illegal content or serious violence against a child, staff must not circulate, copy or forward the material unnecessarily.

- The concern shall be reported promptly to the DSL.

- Relevant technical evidence shall be preserved securely and only to the extent necessary for safeguarding, legal, disciplinary or security purposes.
- Potentially illegal material shall only be disclosed to authorised persons or competent authorities through the appropriate channel.
- IT staff shall not undertake independent investigation of suspected criminal material.
- The school shall record the decision taken, the responsible safeguarding decision-maker and any external referral, subject to applicable confidentiality and data-protection requirements.

35. Monitoring, Filtering and Data Protection

Filtering and monitoring are separate controls. Filtering seeks to prevent access to harmful or inappropriate material; monitoring identifies activity that may require intervention. Both controls shall be risk-based, age-appropriate, proportionate and subject to data-protection governance.

- Before introducing or materially changing monitoring, classroom-screen viewing, behavioural analytics, keyword monitoring, biometric technology, AI monitoring or similar processing, BSGC shall determine the lawful basis and whether a Data Protection Impact Assessment (DPIA) is required. The DPO must be consulted as part of this assessment. The same review applies to existing monitoring where its DPIA status, purpose, scope or risk assessment has not been confirmed.
- *Where Article 35 GDPR requires a DPIA, processing shall not commence or continue until the DPIA has been completed and the required governance approvals have been obtained.*
- The school shall maintain appropriate privacy information explaining what is monitored, purposes, lawful basis, recipients/access, retention, rights and how concerns may be raised.
- Monitoring data shall be accessible only to authorised personnel whose role requires access.
- Monitoring shall not be covert merely because technology makes covert monitoring possible. Any exceptional covert processing shall have a documented legal and safeguarding justification.
- The school shall maintain a Monitoring Data Schedule identifying categories of monitoring data, purpose, lawful basis, authorised access and retention period.
- Monitoring shall be reviewed periodically to ensure that data collected remains necessary and proportionate.
- Suppliers providing monitoring, filtering, MDM, classroom-management, cloud or AI services shall be assessed for data-protection compliance, contractual processor requirements, security, retention and international-transfer implications before approval.

36. Digital Education and Staff Training

BSGC shall provide age-appropriate digital-safety education as part of its wider curriculum and safeguarding programme. Protection through filtering and device controls does not replace education. All staff shall receive training on filtering and monitoring — what BSGC's systems do, staff responsibilities in relation to them, and how to raise a concern — as part of safeguarding induction, with refresher training provided periodically and whenever systems or risks change materially.

- Digital education shall address safe and responsible Internet use, privacy, personal data, passwords and account security, digital identity and reputation, cyberbullying, grooming, sexting, sexual exploitation, harmful content, scams and phishing, misinformation, reporting mechanisms and digital wellbeing.
- The programme shall specifically include the risks created as a result of AI generated and manipulated text, images and videos.

- The programme shall take account of age, maturity, SEND, language needs and individual vulnerability.
- Staff shall receive appropriate training to recognise and respond to online risks and to use filtering, monitoring and classroom-management systems lawfully and appropriately.
- Training shall be refreshed when significant new online risks, technologies or legal requirements arise.

37. Canary Islands Protocols and Local Procedures

BSGC shall take account of applicable Canary Islands educational protocols and guidance when responding to online safety incidents.

- The school's anti-bullying arrangements shall incorporate the applicable Gobierno de Canarias framework for suspected school bullying and cyberbullying.
- The school shall take account of applicable Canary Islands safeguarding protocols for *violence, self-harm, suicide, sexual violence and other relevant risks*.
- *BSGC may participate in or make use of applicable Gobierno de Canarias cybersecurity education and awareness initiatives. The exact title, current status and applicability of any named local protocol must be verified in the legal and regulatory register before it is relied upon.*
- Where a Canary Islands rule or protocol applies specifically to the school's legal status, BSGC shall apply it according to its scope and implementing instructions.

38. Monitoring Data Schedule and Retention

The school shall maintain a separate schedule, approved through data-protection governance, covering retention of digital-safeguarding information. The schedule shall distinguish routine technical/security logs from safeguarding records and shall avoid retaining individual-level monitoring data longer than necessary.

- Routine technical and filtering logs: retained only for the period documented as necessary for security, troubleshooting, safeguarding and audit.
- Safeguarding alerts and case records: retained in accordance with the school's safeguarding record-retention requirements.
- Incident evidence: retained securely for as long as reasonably necessary for the relevant safeguarding, disciplinary, legal or security process.
- Access to retained monitoring information shall be logged or otherwise auditable where technically appropriate.
- At the end of the applicable retention period, information shall be securely deleted or anonymised unless another lawful retention requirement applies.

39. Online Safety Incident Response

All significant online-safety incidents shall follow this sequence:

1. Detect or receive the concern.
2. Protect the student and assess immediate risk.
3. Notify the DSL where safeguarding is implicated.
4. Preserve relevant technical evidence securely without unnecessary copying or circulation.
5. Implement immediate technical controls where required.
6. Determine whether the incident engages a bullying, safeguarding, data-protection, disciplinary or criminal process.

7. Notify parents/carers where appropriate and where doing so does not increase risk.
8. Refer to external authorities where legally required or otherwise appropriate.
9. Record the decision, action taken and outcome.
10. Review whether technical, educational, safeguarding or policy controls need improvement.

40. Legal Compliance Review and Assurance

The annual review of this Policy shall include a documented legal compliance check against the legislation and protocols listed in Section 32.

- The review shall identify changes in law, regulatory guidance, Canary Islands protocols, technology, suppliers and emerging online risks.
- Material changes to monitoring or filtering shall trigger a data-protection review and, where required, a DPIA.
- Governors shall receive assurance that the legal framework, safeguarding arrangements, technical controls and data-protection governance remain effective.
- Any identified legal compliance gap shall have an assigned owner, target date and recorded remediation action.

41. Related BSGC Policies and Procedures

This Policy should be read alongside the following policies:

- Safeguarding and Child Protection Policy
- Data Protection Policy
- Data Protection Procedures
- Acceptable Use Policy
- Staff Digital Expectations Policy
- Digital Learning Policy
- AI Policy
- AI Use and Approval Procedure
- KS5 Personal Device Protocol
- Mobile Phone Policy/Procedure
- Behaviour Policy
- Anti-Bullying Policy