

Version: Approved
Approved date: Sept 2026
Review Date: Aug 2027

The British School of Gran Canaria



Data Protection Policy

Contents

1. Purpose and Rational
 2. Legal and Regulatory Framework
 3. Scope
 4. What is Personal Data?
 5. Special Category and Sensitive Information
 6. Data Protection Principles
 7. Lawful Processing
 8. Transparency and Privacy Notices
 9. Children and Young People's Data
 10. Data Security
 11. Staff Responsibilities
 12. Data Sharing
 13. Third-Party Providers and Educational Technology
 14. Data Protection Impact Assessments
 15. Records of Processing
 16. Retention and Disposal
 17. Individual Data Protection Rights
 18. Subject Access and Other Information Rights Requests
 19. Personal Data Breaches
 20. Photographs, Video and Audio
 21. CCTV, Filtering and Monitoring
 22. Artificial Intelligence
 23. International Transfers
 24. Data Protection and Safeguarding
 25. Training and Awareness
 26. Roles and Responsibilities
 27. Non-Compliance
 28. Monitoring and Review
- Appendix 1 – BSGC Data Protection Principles: Staff Quick Reference

1. Purpose and Rationale

The British School of Gran Canaria recognises that the responsible management and protection of personal information is fundamental to the safety, privacy, dignity and trust of our students, families, staff and wider community.

BSGC collects and processes personal information for a wide range of educational, safeguarding, administrative, employment and operational purposes. The school is committed to ensuring that personal data is collected, used, stored and shared lawfully, fairly, transparently and securely.

This Policy establishes the principles and responsibilities that govern the processing of personal data at BSGC and supports the school's compliance with applicable data-protection legislation.

For GDPR purposes, BSGC will act as the data controller with respect to activities in which the school determines the purposes and means of processing. Third parties that process personal data in accordance with BSGC's documented instructions will act as data processors, unless the nature of the service requires a different legal classification to be documented.

2. Legal and Regulatory Framework

BSGC will comply with applicable data-protection and privacy legislation, including, as applicable:

- EU General Data Protection Regulation (Regulation (EU) 2016/679 – GDPR);
- Spanish Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD);
- Regulation (EU) 2024/1689 on Artificial Intelligence (EU AI Act), where applicable to AI systems used by the school and in accordance with its implementation timeline.
- applicable Spanish legislation relating to education, employment, safeguarding, confidentiality and records;
- applicable requirements concerning international transfers of personal data;
- UK GDPR and the UK Data Protection Act 2018, where applicable to particular processing activities, individuals, services, transfers or contractual arrangements;
- guidance and decisions issued by relevant supervisory authorities, including the Agencia Española de Protección de Datos (AEPD) and, where applicable, the UK Information Commissioner's Office (ICO).

The school will keep its data-protection arrangements under review as legislation and regulatory guidance develop.

3. Scope

This Policy applies to:

- all students;
- parents, carers and families;
- governors;
- teaching and support staff;
- temporary and agency staff;
- volunteers;
- contractors and consultants;
- third-party providers processing information on behalf of BSGC;
- anyone else who has access to BSGC personal data.

It applies to personal data processed:

- electronically or digitally;
- in paper records;
- through school information systems;
- through educational technology and online platforms;
- through email and communication systems;
- through photographs, video and audio;
- through CCTV, access-control and security systems;
- through AI and other emerging technologies;
- on school-owned or authorised personal devices;
- on behalf of the school by third-party organisations.

The Policy applies whether information is processed on school premises, remotely, during school trips or residential visits, or in connection with other school activities.

4. What is Personal Data?

Personal data is information relating to an identified or identifiable living individual. This can include, for example:

- name and contact details;
- date of birth;
- address;
- attendance records;
- academic and assessment information;
- behaviour records;
- photographs and video;
- identification and authentication information;
- communications;
- safeguarding information;
- medical information;
- special educational needs information;
- financial information;
- employment and recruitment records;
- online identifiers and technical information;
- information generated through school systems, filtering and monitoring.

Personal data can exist in both electronic and physical form.

5. Special Category and Sensitive Information

Some personal data requires additional protection because of its particularly sensitive nature. This includes information relating to areas such as:

- health;
- racial or ethnic origin;
- religious or philosophical beliefs;
- biometric information used for identification;
- sexual orientation;
- certain information relating to safeguarding;
- other categories identified by applicable legislation.

BSGC will only process such information where an appropriate lawful basis and additional legal condition applies. Staff must take particular care when accessing, discussing, storing or sharing sensitive information.

6. Data Protection Principles

BSGC will apply the data-protection principles established by applicable law. Personal data must be:

Lawful, fair and transparent - Information must be processed lawfully and individuals should understand how and why their information is being used.

Purpose limited - Information should be collected for specified, explicit and legitimate purposes and not subsequently used incompatibly with those purposes.

Adequate and limited - Only information that is necessary for the intended purpose should be collected and used.

Accurate - Reasonable steps should be taken to ensure information is accurate and kept up to date where necessary.

Stored appropriately - Information should not be retained for longer than necessary.

Secure - Appropriate technical and organisational measures must protect information against unauthorised access, loss, alteration, disclosure or destruction.

Accountable - BSGC must be able to demonstrate that it complies with these principles.

Data protection by design and by default – Privacy shall be integrated from the outset of projects and, by default, only data strictly necessary for each intended purpose shall be processed, with access and retention periods restricted accordingly.

7. Lawful Processing

BSGC will only process personal data where an appropriate lawful basis exists. Depending on the circumstances, this may include:

- legal obligation
- Performance of a contract with the data subject or the implementation of pre-contractual measures at their request;
- Performance of a task carried out in the public interest or in the exercise of official authority, where an applicable legal basis exists;
- Protection of the vital interests of the data subject or another natural person;
- Legitimate interests, where applicable;
- consent, where appropriate.

Consent will not automatically be used simply because it is convenient. Where consent is relied upon, it must be appropriately obtained, informed and capable of being withdrawn, subject to applicable legal requirements.

In the case of special categories of data, BSGC shall identify, in addition to a legal basis under Article 6 of the GDPR, an applicable condition under Article 9(2). Data relating to criminal convictions and offences shall only be processed in accordance with the terms of Article 10 of the GDPR and applicable Spanish law

Staff must not assume that they can use personal information simply because the school already holds it.

8. Transparency and Privacy Notices

BSGC will provide appropriate privacy information to individuals explaining:

- the identity and contact details of BSGC as data controller;
- the contact details of the Data Protection Officer (DPO);
- the purposes of the processing and, where applicable, the categories of personal data concerned;
- the legal basis for the processing and, where legitimate interests are relied upon, the legitimate interests pursued;
- the recipients or categories of recipients of the personal data;
- any intended international transfers and the applicable transfer mechanism or safeguards;
- the retention period or, where that is not possible, the criteria used to determine that period;
- the applicable rights, including the right to withdraw consent where processing is based on consent, and the right to lodge a complaint with the AEPD (Spanish Data Protection Authority);
- where the personal data are not obtained directly from the data subject, the categories of personal data and the source from which they originate; and, where applicable, the existence of automated decision-making or profiling together with the meaningful information required by the GDPR;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, and the possible consequences of failure to provide such data.

Privacy information will be provided in an accessible and age-appropriate manner, particularly for students.

Privacy notices will be reviewed regularly and whenever there are significant changes to the school's processing activities.

9. Children and Young People's Data

BSGC recognises that students require particular care and protection when their personal information is processed. The school will:

- consider the age and understanding of students when explaining data use;
- provide appropriate and accessible privacy information;
- ensure that children's information is processed fairly and proportionately;
- apply appropriate safeguards to educational technology;
- carefully consider the risks associated with profiling, monitoring and automated processing;
- take additional care when introducing new technologies involving children's data.

The school will consider relevant regulatory guidance concerning children's personal information and educational technology.

In Spain, where processing is based on a minor's consent, pupils aged 14 and over may provide consent on their own behalf, except where the law requires the assistance of those exercising parental authority or guardianship for the specific act in question. For minors under the age of 14, processing based on consent shall only be lawful if consent is provided by the holder of parental authority or guardianship. This rule does not imply that all processing of pupil personal data must rely on consent.

10. Data Security

BSGC will implement appropriate technical and organisational measures to protect personal information. These may include:

- access controls;
- passwords and authentication;
- role-based permissions;
- encryption where appropriate;
- secure networks;
- managed devices;
- filtering and monitoring;
- secure backups;
- malware and endpoint protection;
- physical security;
- secure disposal;
- staff training;
- incident management.

Access to personal information will be based on legitimate need and appropriate authorisation. Staff must not access information simply because they technically have the ability to do so.

11. Staff Responsibilities

Everyone who handles personal data on behalf of BSGC has a responsibility to protect it. Staff must:

- use personal information only for legitimate school purposes;
- access only information they need for their role;
- keep information secure;
- avoid unnecessary copying or downloading;
- use approved school systems;
- follow retention and disposal requirements;
- check recipients before sending information;
- use appropriate care when discussing confidential matters;
- report suspected breaches promptly;
- complete required data-protection training.

Staff must not:

- share passwords;
- leave confidential information unattended;
- send personal information to unauthorised recipients;
- use personal email accounts for confidential school information;
- store school information on unauthorised devices or services;
- upload confidential information to unapproved AI tools;
- disclose information to parents or third parties without appropriate authority.

12. Data Sharing

BSGC may share personal information where there is a lawful basis and appropriate justification.

Information may be shared with, for example:

- government or regulatory authorities;
- educational institutions;
- examination and awarding bodies;
- healthcare or safeguarding professionals;

- service providers;
- insurers;
- legal or professional advisers;
- other organisations where required or permitted by law.

BSGC will apply the principles of necessity, proportionality and data minimisation when sharing information. Where appropriate, formal data-sharing or data-processing arrangements will be established.

13. Third-Party Providers and Educational Technology

Before introducing a service that processes personal information on behalf of BSGC, the school will consider:

- the purpose and necessity of processing;
- the data involved;
- the provider's security arrangements;
- contractual terms;
- data-processing arrangements;
- international transfers;
- data retention;
- sub-processors;
- deletion arrangements;
- the provider's use of data for analytics, profiling or AI training;
- risks to students and staff.

Where appropriate, a Data Protection Impact Assessment (DPIA) will be completed before processing begins. Current school guidance identifies DPIAs as particularly important where processing is likely to create a high risk to individuals' rights and freedoms and recommends reassessment when significant changes occur.

Third-party providers must sign a Data Processing Agreement, whenever possible.

Where a supplier acts as a data processor, the relationship must be formalized through a contract or other binding legal act pursuant to Article 28 of the GDPR, containing the mandatory minimum provisions, prior to the supplier accessing any personal data.

Prior to engagement, BSGC shall carry out and document the necessary due diligence to verify that the supplier provides sufficient guarantees in accordance with Article 28(1) of the GDPR and Recital 81, including security measures, sub-processors, data location, international transfers, retention, return or deletion of data, and audit capabilities.

The supplier shall not use BSGC data for its own purposes, advertising, profiling, or the training of AI models, unless such purpose, the supplier's legal role, and the corresponding legal basis have been thoroughly assessed and expressly authorized by BSGC

14. Data Protection Impact Assessments

The obligation to carry out a DPIA rests with BSGC as the data controller. The practical drafting may involve internal or external support, including engaged consultants, but BSGC shall remain responsible for ensuring its proper completion, implementing the resulting measures, and documenting the decision. The DPO shall be consulted and shall monitor the implementation of the DPIA. A DPIA shall be conducted prior to the processing when it is likely to result in a high risk to the rights and freedoms of individuals, particularly when introducing:

- new technologies;
- significant monitoring systems;
- AI systems;
- large-scale processing;
- systems involving sensitive information;
- new forms of profiling or automated decision-making;
- significant changes to existing processing.

A DPIA must identify:

- the purpose of the processing;
- the information involved;
- the data subjects affected;
- the legal basis;
- the potential risks;
- the measures to mitigate those risks;
- the residual risks;

the documented decision of BSGC on whether to proceed, specifying any applicable conditions and mitigation measures.

If the DPIA concludes that a high risk persists that cannot be reasonably mitigated, BSGC shall consult the AEPD prior to commencing the processing, in accordance with Article 36 of the GDPR.

15. Records of Processing

BSGC shall maintain an up-to-date Record of Processing Activities in accordance with Article 30 of the GDPR. The record shall identify, as appropriate, categories of personal data;

- categories of data subjects;
- purposes of processing;
- lawful bases;
- recipients;
- international transfers;
- retention periods;
- security measures;
- relevant systems and third parties.

A Record of Processing Activities is an important accountability mechanism and is specifically identified in current school data-protection guidance.

16. Retention and Disposal

BSGC will retain personal information only for as long as necessary or as required by law, regulation, contractual requirements or legitimate school purposes.

The school will maintain an appropriate Data Retention and Disposal Schedule.

When information is no longer required, it will be securely:

- deleted;
- destroyed;
- otherwise disposed of.

Particular care will be taken when disposing of paper records, computers, storage devices and other equipment containing personal information.

17. Individual Data Protection Rights

Subject to applicable legal requirements, individuals may have rights including:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object;
- rights concerning automated decision-making and profiling.

The availability of a specific right depends on the circumstances and the legal basis of the processing. BSGC shall facilitate the exercise of these rights free of charge, except in the exceptional circumstances provided for in the GDPR, and shall respond without undue delay and, in any event, within one month of receipt. Where applicable, this period may be extended by two further months where necessary, taking into account the complexity and number of the requests, informing the data subject within the initial month. Data subjects may lodge a complaint with the AEPD.

18. Subject Access and Other Information Rights Requests

Requests regarding personal data must be forwarded without delay to the designated internal channel and to the DPO for advice. Responsibility for responding and complying with statutory deadlines rests with BSGC as the data controller. Staff must not respond to, refuse, alter, or delete any information on their own initiative when faced with a request. This includes requests that may appear informal, such as: *'Can I see everything the school has about my child?'* Such requests may constitute an exercise of information rights and should therefore be referred appropriately.

19. Personal Data Breaches

A personal data breach may include:

- loss or theft of a device;
- sending information to the wrong person;
- unauthorised access;
- accidental disclosure;
- hacking;
- phishing;
- malware or ransomware;
- inappropriate sharing;
- loss of paper records;
- accidental deletion where information cannot be recovered.

Any suspected personal data breach must be reported immediately via the BSGC Data Breach Procedure. Staff must not delay notification due to uncertainty over whether an incident constitutes a breach. The DPO shall provide advice on risk assessment and notification obligations; however, the ultimate decision and legal responsibility rest with BSGC as the data controller. Where the breach is likely to result in a risk to individuals' rights and freedoms, it shall be notified to the supervisory authority without undue delay and, where feasible, within 72 hours of BSGC becoming aware of it. Where a high risk is likely, it shall also be communicated to the affected data subjects without undue delay, unless a statutory exemption applies.

20. Photographs, Video and Audio

Photographs, video and audio recordings that identify individuals constitute personal data. BSGC will ensure that the collection and use of images and recordings is lawful, proportionate and transparent.

Particular care will be taken with:

- school websites;
- social media;
- promotional materials;
- performances;
- sporting events;
- school trips;
- CCTV;
- student work;
- recordings involving children.

Current school guidance similarly identifies photographs and videos of identifiable individuals as personal data requiring an appropriate lawful basis.

21. CCTV, Filtering and Monitoring

Where BSGC uses CCTV, network monitoring, content filtering, device management, and other digital monitoring systems, these shall be operated lawfully, proportionately, and transparently. The school shall:

- identify the specific purpose of the monitoring;
- restrict access to monitoring data and logs;
- in the case of security CCTV, delete footage within a maximum period of one month from its recording, unless it must be retained to evidence incidents in accordance with the LOPDGDD;
- provide appropriate privacy information and, for CCTV, install prominent signage ensuring easy access to the information required under Article 13 of the GDPR;
- train authorized personnel;
- conduct a DPIA where required;
- refrain from installing cameras in toilets, changing rooms, or staff break areas; monitoring inside classrooms or other particularly intrusive areas shall only be considered on an exceptional, necessary, and proportionate basis.

Monitoring shall not be deployed merely because the technology enables it.

Where monitoring affects staff, workplace privacy rights and the duty of prior notice shall also be strictly observed. Audio recording shall remain strictly exceptional and shall only be implemented where there is a specific, necessary, and proportionate justification.

22. Artificial Intelligence

AI tools can pose significant risks to personal data and fundamental rights. Accordingly, BSGC shall enforce the requirements set out in its Artificial Intelligence Policy and AI Use and Approval Procedure, conduct the applicable prior data protection assessment, and evaluate obligations under Regulation (EU) 2024/1689 (EU AI Act) in line with its implementation timeline. Staff and pupils must not enter personal, confidential, safeguarding, or other sensitive information into unapproved AI tools.

Where AI is deployed to support educational or administrative activities, BSGC shall take into account:

- necessity;
- accuracy;
- transparency;
- data protection;
- safeguarding;
- bias;
- human oversight;
- age appropriateness;
- security.

AI must not replace appropriate professional judgement in significant decisions concerning pupils or staff. No decision shall be taken based solely on automated processing that produces legal effects or similarly significantly affects an individual, unless a lawful exception under Article 22 of the GDPR applies and the requisite safeguards are implemented, including meaningful human intervention where appropriate.

23. International Transfers

BSGC shall comply with the requirements set out in Articles 44 to 49 of the GDPR where personal data are transferred outside the European Economic Area (EEA), including remote access from a third country where such access constitutes a transfer. Prior to any transfer, the country of destination, the data importer, and any sub-processors shall be identified, and the applicable transfer mechanism shall be documented: an adequacy decision; appropriate safeguards under Article 46—including, where applicable, Standard Contractual Clauses (SCCs) and a Transfer Impact Assessment (TIA) accompanied by supplementary measures; or, exceptionally, a derogation under Article 49. Particular attention shall be paid to cloud services, educational technology (EdTech), and AI platforms.

Where the UK GDPR applies by virtue of its territorial scope or a specific processing activity, BSGC shall assess and document the relevant UK requirements separately, without prejudice to its ongoing obligations under the EU GDPR

24. Data Protection and Safeguarding

Data protection and safeguarding are closely connected. BSGC will not use data-protection requirements as a reason to prevent appropriate safeguarding action where information needs to be shared to protect a child or another individual. At the same time, safeguarding information must be handled with appropriate confidentiality and security. Staff should seek advice from the Designated Safeguarding Lead (DSL) and DPO where there is uncertainty about sharing safeguarding information.

25. Training and Awareness

BSGC will provide appropriate data-protection training to staff and relevant volunteers. Training should cover:

- basic data-protection principles;
- confidentiality;
- secure use of systems;
- phishing and cybersecurity;
- personal data breaches;
- data-subject rights;
- safeguarding information;
- use of photographs and recordings;
- AI and educational technology;
- secure communication;
- reporting procedures.

Training will be provided on induction and refreshed periodically, with additional training where roles or risks require it.

26. Roles and Responsibilities

Governing Body - The Governing Body provides oversight and assurance that appropriate data-protection arrangements are in place.

Headteacher - The Headteacher has overall operational responsibility for ensuring that the school implements this Policy and maintains an effective data-protection culture.

Director of Operations - The Director of Operations supports the implementation of data-protection arrangements across the school's operational functions and ensures that relevant procedures and controls are maintained.

Data Protection Officer - The DPO will:

- advise BSGC on data-protection obligations;
- monitor compliance;
- advise on DPIAs;
- support data-protection audits;
- advise on data breaches;
- support information-rights requests;
- advise on policies and procedures;
- act as an appropriate point of contact with the supervisory authority where required.

The DPO shall be involved, properly and in a timely manner, in all issues relating to the protection of personal data, shall act independently, and shall not receive any instructions regarding the exercise of their tasks. The DPO shall be provided with adequate resources, access to processing operations, and direct reporting access to the highest management level; any other duties assigned shall not give rise to a conflict of interest. Their contact details shall be published and communicated to the AEPD. The DPO shall inform and advise, monitor compliance, provide advice regarding DPIAs, and act as the contact point for the supervisory authority, without assuming the corporate accountability that rests with BSGC.

Data Protection Consultants – BSGC may engage an external company to provide specialized support with audits, breach management, DPIAs, and related matters. Such support shall not transfer BSGC's compliance accountability. Where the external provider also delivers external DPO services, the independence, absence of conflicts of interest, and statutory duties set out in Articles 38 and 39 of the GDPR shall be strictly upheld. The material execution of DPIAs or investigations by consultants does not alter the fact that all decisions and legal accountability remain with BSGC.

IT Manager - The IT Manager is responsible for appropriate technical controls, including:

- access management;
- cybersecurity;
- device security;
- backups;
- system configuration;
- technical monitoring;
- security incident response.

Designated Safeguarding Lead - The DSL is responsible for ensuring that data-protection considerations support rather than impede effective safeguarding.

All Staff - All staff are responsible for protecting personal information and following BSGC procedures, with everyone working in a school having responsibility for protecting personal data, not just the DPO.

27. Non-Compliance

Failure to comply with this Policy may result in:

- additional training;
- restriction of access to information or systems;
- management action;
- disciplinary action where appropriate;
- referral under safeguarding procedures;
- notification to relevant authorities where required.

The school's response will be proportionate to the nature and seriousness of the incident. Deliberate or reckless misuse of personal information will be treated particularly seriously.

28. Monitoring and Review

BSGC will monitor compliance through appropriate measures including:

- review of subject access and other rights requests;
- review of third-party providers;
- staff training records;
- review of access permissions;
- review of retention arrangements;
- periodic review of the Record of Processing Activities.

The Policy will be reviewed at least annually and sooner where there are significant changes to legislation, regulatory guidance, technology or school practice.

Appendix 1 – BSGC Data Protection Principles: Staff Quick Reference

The checklist below is an aid to help make this important policy practical and accessible to all staff.

Before you use personal information, ask:

1. Do I need it?

Only use information that is necessary.

2. Am I allowed to use it?

Make sure there is a lawful basis.

3. Does the person know?

Consider whether the use is covered by the school's privacy information.

4. Is it accurate?

Check important information.

5. Who needs to see it?

Share only with authorised people who need it.

6. Is it secure?

Use approved systems and protect devices, passwords and documents.

7. How long should I keep it?

Do not retain information unnecessarily.

8. What if something goes wrong?

Report it immediately—don't wait to find out whether it is "really" a breach.