Version:	Final
Date approved:	27.10.2022
Next scheduled review:	September 2024

The British School of Gran Canaria
Online Safety Policy
Policy Document

Index

THE BRITISH SCHOOL OF GRAN CANARIA

ONLINE SAFETY POLICY

1. Definitions

Throughout this document the following words, terms and phrases have the following meanings:

BSGC – British School of Gran Canaria, also referred to as the School.

Pupils – include the term children and students.

School – includes both the Tafira and South School sites.

School community – includes all pupils and employees.

Governor – a member of the elected representative who have oversight of the school.

Senior teacher – member of the SMT.

SMT – Senior Management Team.

Head – the person with day-to-day and strategic responsibility, along with the senior leaders, for the running of the school.

Online Safety Coordinator – the assigned person within the school with this responsibility

Staff - includes all employees of the school, i.e. teachers, administrators, canteen workers and ancillary personnel.

Network Manager – Senior IT Technician employed by the school

Data Manager – Contracted manager, currently Prodat.

2. Rationale

This Online Safety Policy explains how BSGC will help its pupils and school personnel to be responsible users and remain safe while using the Internet and other communications technologies for educational, personal and recreational use.
This policy will:

- clarify behaviour expectations and codes of practice for the responsible use of for use technologies and access to the internet.
- provide protection and safeguarding for BSGC pupils and staff when working online and/or electronically by establishing clear procedures to reduce the chances of harm and how to address online abuse.
- ensure all BSGC members are aware that unlawful or unsafe behaviours are unacceptable and outline the consequence of inappropriate actions.

3. Scope of the Policy

This policy outlines the role of the school in ensuring that pupils are kept safe on-line in school.

Although the school will take preventative steps to stop pupils being exposed to risk while online during school time, we also recognise the extensive and pervasive nature of Internet outside school. Pupils will, therefore, be educated of the potential risk of Internet use, and the need to acquire skills and strategies to keep themselves safe.

Additionally, this document:

- Identifies the key people and their roles and responsibilities.
- Outlines the strategy in which the school will endeavour to keep its pupils safe from harm, both by electronic protection, and by education of pupils, staff and parents.
- Identifies the procedures to follow in the case of an incident.

4. Roles and responsibilities

Online Safety Governor

The Appointed Online Safety Governor is Debbie Davies. Their role includes:

- Meeting with the Online Safety Co-ordinator on a regular basis.
- Complete a termly Monitoring Visit, including a review of Online Safety incident logs.
- Regular monitoring of filtering/change control logs.
- Reporting updates, information and issues to the Governors' monthly meetings.

Online Safety Coordinator

The Online Safety Coordinator is Ryan Hannah. This role includes:

- Day-to-day responsibility for advice and guidance on Online Safety issues, and taking a leading role in establishing and reviewing the school Online Safety policies and documentation.
- Ensuring that all staff are aware of the policy and the procedures that need to be followed in the event of an Online Safety incident taking place.
- Providing training and advice for staff.
- Liaising with the *Inspección de Educación* and other agencies if and when required.
- Liaising with BSGC ICT Support staff on Online Safety.
- Receiving reports of Online Safety incidents and maintaining a log of incidents to inform future Online Safety Policy and practice.
- Liaising with Online Safety Governor.

Head

The Head has overall responsibility for ensuring the safety of the school community. However, the day-to-day responsibility for Online Safety is delegated to the Online Safety Lead.

The Headteacher will work with the Online Safety Coordinator to ensure that pupils are kept safe, and made aware of the potential for serious child protection issues to arise from:

- sharing of personal data;
- access to illegal / inappropriate materials;
- inappropriate on-line contact with adults / strangers;
- potential or actual incidents of grooming;
- cyber-bullying.

Network Manager

Has responsibility for

- monitoring, adapting and controlling the school ICT systems, servers, hardware, software and protective barriers to ensure that users, the systems and equipment are safe.
- controlling, filtering and monitoring access of school users to the internet.
- monitoring and preventing unwanted and unauthorised access to school system from outside.
- ensuring the school is adequately protected should any unwanted threats.
- briefing and updating the Online Safety Governor, Online Safety Lead, and Head of issues and actions required to keep the school, and all its users, safe, protected and fully informed.

5. Education for children

Keeping children safe online is crucial and central to all aspects of education. Although filters are in place to protect pupils whilst in school, this is only a small percentage of the time that a child is potentially online. Schools must play their part in educating children in how to negotiate the internet without the school's filters and firewalls in place. BSGC will do everything possible to develop pupils' risk strategies and responses to threats, whether potential or real.

BSGC will provide Online Safety education in the following ways:

- a planned Online Safety programme as part of Computer Science/ PHSE /other lessons, with key themes regularly revisited across the curriculum, with all staff playing an important role;
- key Online Safety messages will be reinforced as part of a planned programme of assemblies;
- children will be taught in all lessons to be critically aware that not everything they access online is truthful or valid and be taught to check the accuracy of information;
- children will be encouraged to adopt and promote safe and responsible use of ICT, the internet and mobile devices, within and outside school;
- children will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- rules for use of ICT systems and the internet will be posted in all rooms, as the use of mobile devices means that the Internet is accessible in all areas of the school;
- staff will act as positive and strong role models in their use of ICT, the internet and mobile devices.

6. Education for Parents / Carers

Educating parents is key if children are to develop strategies to deal with the potential risks of the internet. Parent's perception of risk may be limited or not fully informed. Scare stories in the media often cause parents unnecessary concerns, whilst obscuring real issues and risks. The school will attempt to provide as much useful information as possible to help parents keep their children safe online outside of the school. This information will be available to extended family, such as grandparents, as well. This is achieved via

- social media;
- letters, newsletters, web site;
- parents' meetings or workshops.

All members of staff can provide support to parents but they have an obligation to refer any contact if they suspect that there may be Online Safety concerns.

7. Education and Training for Staff

It is essential that all staff receive Online Safety training and understand their responsibilities as outlined in this policy. Training will include:

- a planned programme of formal Online safety training;
- the BSGC Online safety Policy will be presented to and discussed by staff on an annual basis;
- the school will seek to provide the best, updated advice to support Online Safety practices for individuals and groups.

8. E-Security

The School will take all reasonable steps to maintain a safe and secure environment. To this end:

- school ICT systems will be managed in ways that ensure that the school meets the Online Safety technical requirements outlined by Spanish authorities and recommendations of UK guidance.
- regularly review and audit the safety and security of school ICT systems;
- servers, wireless systems and cabling must be securely located and physical access restricted;
- all users will have clearly defined access rights to school ICT systems;
- all users will sign the school's 'Acceptable Use of Technology Expectations' before using the Internet;
- the master/administrator passwords for the school ICT system used by the Network Manager must also be available to the Headteacher or another nominated senior leader and kept in a secure place;
- in the event of ICT Support (or other persons) needing to switch off the filtering for any reason, this must be logged and carried out by a process that is agreed by the Head;
- any filtering issues should be reported immediately to the Head.
- requests from staff for sites to be removed from the filtered list will be considered by the Head;
- IT Support staff will regularly monitor and record the activity of users on the school ICT systems, with users being made aware of this monitoring in the Acceptable Use of Technology Expectations;
- any actual/potential Online Safety incident must be reported to the relevant person(s) which in most cases will include the Online Safety co-ordinator, unless there are concerns about their conduct, in which case it should be escalated to involve SMT or the Head;
- the school infrastructure and individual workstations are protected by up-to-date virus software;
- personal data must not be sent over the internet or taken off the school site without prior approval and only done so in a secured and encrypted manner.

The use of digital imaging technologies has significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff and children must be aware of the risks associated with sharing images and with posting digital images on the internet. Such images may remain available on the internet as part of a digital footprint, and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

Staff must be aware of, and understand, the school's policy on staff use of social networks as outlined below:

- when using digital images, staff must educate pupils about the risks associated with the taking, using, sharing, publication and distribution of images. In particular, recognition of the risks attached to publishing one's own images on the internet e.g., on social networks.

- staff can take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images, in part related to GDPR authorisation. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- care should be taken when taking digital/video images that children are dressed appropriately and not participating in activities that might bring the individuals or the school into disrepute;
- children must not take, use, share, publish or distribute images taken in school, of others, without explicit permission of their teacher and the school;
- photographs published on the website, or elsewhere, that include children, will be selected carefully and will comply with good practice guidance on the use of such images and ensuring GDPR authorisation;
- children's full names will not be used anywhere on a website, social media or blog, particularly in association with photographs;
- GDPR authorisation from parents or carers will be obtained before photographs of children are published on the school website or social media.

9. Data Protection

Personal data will be recorded, processed, transferred and made available according to the *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos (juridicas.com)* which states that personal data must be:

- fairly and lawfully processed,
- processed for limited purposes,
- adequate, relevant and not excessive,
- accurate,
- kept no longer than is necessary,
- processed in accordance with the data subject's rights,
- secure,
- only transferred to others with adequate protection.

Staff must ensure that they take care at all times to ensure the safe-keeping of any critical data, minimising the risk of its loss or misuse. They must store personal or critical data only on secure password protected BSGC computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

10. Managing the ICT Infrastructure

Internet access, security, virus protection and filtering

BSGC manages the ICT infrastructure by applying a variety of safeguards. This is the responsibility of the Network manager and Online Safety Coordinator to keep up to date and current.

All users also have the responsibility to use the internet and school systems safely, informing the Network Manager if spam, phishing, malware, ransomware and virus attachments are identified or suspected.

BSGC Email

The School provides all staff with an email account for use in connection with their duties. It is expected that such email users recognise that they are representing the school in any correspondence they undertake via this system and therefore have a duty to act with due care and regard to their actions.

Users of the school email should be aware of the following:

- the school email system may be regarded as safe and secure. It is virus checked and monitored, and should be used in all school related communications.
- school email accounts must not be used for private communications.
- e-mail and internet communications may be monitored.
- all users must immediately report to the nominated person, identified in this policy, of the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature - users must not respond to any such email.
- any digital communication between staff and pupils or parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school systems.
- personal e-mail addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- children will be taught about good social media and email practices, safety issues, and how to respond to the risks attached to the use of such media.
- On leaving the school, staff access to the school's email account and data bases will stop.
- BSGC reserves the right to contact the Police if one of our staff or pupils receives an email that we consider is particularly disturbing or breaks the law;

Password policy

- Pupils must always keep their password private, must not share it with others and must not leave it where others can find it.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

School website

- The Head takes overall responsibility to ensure that the website content is accurate and presentation quality is maintained, while delegating day-to-day responsibility to the school's website coordinator.
- Most material is the school's own work but where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- The points of contact on the website are the school address, telephone number and email address. Home information or individual e-mail identities are not published.
- Photographs published on the website do not have names attached and have relevant parental and GDPR permissions archived.

Social Media

- Only BSGC official social media accounts will be used to promote the school, share information and celebrate achievement within the BSGC community.
- Any photographs or information must not contain details that may allow identification by unknown individuals.
- All relevant GDPR and parental permissions are needed for publication and sharing of information on BSGC social media.
- An assigned member of staff will be responsible for collecting information and making the daily posts to these accounts.

11. Illegal and unacceptable internet activity

The activities below are illegal, or are considered unacceptable in a school context and, therefore, users of the school systems must not engage in these activities. In this regard, school policies and systems restrict and forbid certain Internet usage. Users must not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images;
- promotion or conduct of illegal acts e.g. under safeguarding/child protection, obscenity, computer misuse and fraud legislation;
- adult material that potentially breaches Spanish or UK Obscene Publications Laws or regulations;
- racist material;
- pornography;
- promotion of any kind of discrimination;
- promotion of racial or religious hatred;
- threatening behaviours, including promotion of physical violence or mental harm;
- any other information which may be offensive or breaches the integrity or the ethos of the school;
- using school systems to run a private business;
- use of systems, applications, websites or other mechanisms that bypass filters, firewalls or other safeguards;
- uploading, downloading or transmitting commercial software or other copyrighted materials belonging to third parties, without the necessary licensing permissions.
- revealing or publicising confidential or proprietary information e.g. financial / personal information, databases, computer / network access codes and passwords.
- creating or propagating computer viruses or other harmful files;
- carrying out sustained or instantaneous high volume network traffic e.g. downloading /uploading files that causes network congestion and hinders others in their use of the internet;
- streaming or downloading from sites such as Netflix, Spotify;
- non-educational online gaming;
- online gambling;
- publishing to YouTube or similar sites, unless for educational reasons and with prior permission from Head of Sector and the GDPR Lead.

12. Responding to incidents of misuse

All members of the school community are committed to the responsible use of ICT and follow this policy. If an infringement of the policy takes place, through careless, irresponsible or deliberate misuse, user misconduct should be reported to the Online Safety Lead and the process for reporting incidents followed accordingly as for any aspect of child safety or welfare or staff misconduct.

Expected Conduct

The BSGC community are expected to:

- use the school ICT systems in accordance with the Acceptable Use Policy;
- understand the importance of adopting good Online Safety practice at all times;
- acknowledge and understand the consequences of misuse or access to inappropriate materials;
- recognise and report instances of information abuse, misuse or access of inappropriate materials;
- acknowledge and adhere to the policy on the use of hand-held devices and understand how these policies relate to taking / use of images and cyber-bullying;

In addition, staff are required to read the school's Online Safety Policy, agree to, and comply with the expectations. Similarly, all pupils will be guided on safe and responsible use of the internet and electronic devices and students in Year 5 and above are expected to sign, each year, the Acceptable use of Technology Agreement. They will also have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents/Carers will be provided with information on safe use of the Internet, school expectations on 'acceptable use' and the sanctions that might result from their misuse.

Incident Management

BSGC will:

- closely monitor and apply the Online Safety Policy, applying differentiated sanctions when required;
- encourage community members to be vigilant in reporting issues, confident that issues will be dealt with quickly and sensitively, and ensure staff are aware of the Whistleblowing policy;
- implement a continuous cycle of enhancement of the policy to ensure it keeps abreast of technological advances;
- inform parents/carers of those involved in Online safety incidents;
- contact the Police if one of our staff or pupils receives or sends online communication that we consider are particularly disturbing or break the law.

Handling complaints

The school will take reasonable precautions to ensure Online Safety. It is not possible to guarantee that unsuitable material can never appear on a school computer or hand-held device, nor that negative incidents or interactions do not occur, and the school cannot accept liability for material accessed, or any consequences of Internet access if it has acted to ensure safety and minimise risk.

The School Community is given information about unacceptable use and possible sanctions which may include:

- interview/counselling by a member of staff;
- informing parents or carers;
- sanctioning in line with the school' Discipline and Sanctions Policy;
- removal of Internet or computer access for a period;
- referral to Police.
- The Online Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head directly as set out in the Whistleblowing Policy.
- Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy.

Appendix A – Management of ICT Infrastructure

This school:

- has educational, filtered, secure broadband connectivity to the Internet;
- ensures network health through use of an anti-virus software;
- blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- blocks pupil access to music download or shopping sites – except those approved for educational purposes;
- is vigilant in its supervision of pupils' ICT use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- ensures all staff and pupils in Year 5 and above have signed an acceptable use agreement form and understand that they must report any concerns;
- requires staff to preview websites before use and encourages use of the school's Learning Platform as a key way to direct pupils to age and subject appropriate web sites;
- is vigilant when conducting image searches with pupils, e.g., Google image search;
- informs all users that Internet use is monitored;
- informs staff and pupils that that they must report any failure of the filtering systems directly to the system manager;
- makes clear through staff meetings and teaching programmes that all users know and understand the 'rules of appropriate use' and the sanctions that result from misuse;
- provides advice and information on reporting offensive materials, abuse/ bullying etc. to pupils, staff and parents;
- reserves the right to refer any material we suspect is illegal to the appropriate authorities, e.g., the Police.

Appendix B – Acceptable Use of Technology Agreements

1. BSGC Acceptable Use of Technology Expectations (Parents)

Introduction

BSGC recognises that the use of technology enhances students' opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and global citizenship. We are committed to helping students to access and use technology appropriately, including their personal responsibility.

The school's technological resources, including email and Internet access, are provided for educational purposes. Technology users are expected to comply with BSGC rules, act responsibly and honour the terms and conditions set by the teaching staff, and identified within the Acceptable Use Policy agreed with each pupil. The Acceptable Use Policy outlines the guidelines and behaviours expected by all users of the school's technologies or when using personally owned devices on the school's campuses:

- The BSGC network is intended for educational purposes.
- Technologies and devices covered by the policy include Internet access, desktop computers, mobile computers or devices, video conferencing, online collaboration apps, message boards, social media and email.
- Activity over the school's network may be monitored and retained.
- Access to online content via the network is restricted in accordance with school policies and firewalls.
- Students are expected to behave appropriately and respectfully online, as they would in person.
- Misuse of school resources may result in disciplinary action.
- All users are responsible for their use of technology and agree to make every effort to avoid inappropriate content.
- Users must alert BSGC staff immediately of any concerns for safety or security.
- This Acceptable Use Policy applies to school-owned technology equipment and privately owned devices accessing the school's network, while on the school's sites, transport, trips or events.

In order to be effective in the application of our expectations, and to ensure that similar expectations apply at home and in school, the following guidelines are shared with all BSGC parents.

BSGC looks to parents for support with the following expectations:

1. *Support the positive use of technology as part of daily school life and as an integral tool for teaching and learning.*

2. *Promote and model the safe use of technology and the internet.*

3. *Monitor your child's social media use and support the school's social media expectations.*

4. *Support the school's online safety expectations and Acceptable Use Policy.*

This agreement is in place to ensure all children enrolled at BSGC are kept safe while online. If you have any further questions or would like additional advice, please contact your child's Head of Sector.

2. BSGC Acceptable Use of Technology Agreement (Secondary)

All users must read and sign that they are in agreement with, and will follow the Acceptable Use Policy.

Acceptable Use - I will:

- Use school technologies for school-related activities.
- Follow the same expectations for respectful and responsible behaviour online that I am expected to follow offline.
- Treat school resources carefully, and alert staff if there is any problem with them.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a member of staff if I see threatening, inappropriate, or harmful content (images, messages, and posts) online.
- Use school technologies at appropriate times, in approved places, for educational pursuits.
- Cite sources when using online sites and resources for research.
- Be cautious in the protection of the safety of my own safety and that of others.
- Help to protect the security of school resources.

Unacceptable Use - I will not:

- Use school technologies in a way that could be personally or physically harmful.
- Attempt to find inappropriate images or content. (The intent to seek inappropriate images or content is a violation of this Acceptable Use Policy.)
- Engage in cyber bullying, harassment, or disrespectful conduct toward others.
- Try to find ways to circumvent the school's firewalls and filters. (The intent to circumvent safety measures is a violation of this Acceptable Use Policy.)
- Use school technologies to send spam or chain mail.
- Post or otherwise disclose personally-identifying information about myself or others.
- Agree to meet someone I meet online in real life.
- Use language online that would be unacceptable in the classroom.
- Use school technologies for illegal or inappropriate activities.
- Attempt to hack or access sites, servers, or content that is not intended for my use.

This is not an exhaustive list. All users must use their own good judgment when using school technologies.

Violations of the Acceptable Use Policy - Violations may have disciplinary consequences, including:

- Suspension of network, technology, or computer privileges;
- Notification to parents;
- Detention or suspension from school and school-related activities;
- Legal action and/or prosecution.

I acknowledge the policy, the points identified in this declaration, and agree to follow and uphold the spirit and specific guidelines detailed.

Signed Date

3. BSGC Acceptable Use of Technology Agreement (Primary)

All students must read and sign that they understand the information below and agree to follow the rules.

Acceptable Use - I will:

- Use the computer or tablet for schoolwork only.
- Take care of all equipment.
- Only visit web sites and apps that my teacher asks me to.
- Tell a teacher if I am unhappy with something I see or receive messages I do not like.
- Ask for help if I am unsure.

Unacceptable Use - I will not:

- Take part in Cyber Bullying.
- Use the computer or tablet to chat or send messages.
- Share personal information online.
- Use bad or kind words.
- Meet strangers from the internet or talk online to people I don't know.

I understand that when using a computer or tablet I must make good decisions.

I understand that if I deliberately break these rules, I could be stopped from using the internet, computers and tablets, and my parents will be contacted.

Signed Date

4. BSGC Acceptable Use of Technology Agreement (Staff and Visitors)

All users must read and sign that they are in agreement with, and will follow the Acceptable Use Policy.

Acceptable Use - I will:

- Use school technologies for school-related activities.
- Follow the same expectations for respectful and responsible behaviour online that I am expected to follow offline.
- Treat school resources carefully, and alert ICT Department if there is any problem with them.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert the Online Safety Lead if I see threatening, inappropriate, or harmful content (images, messages, and posts) online.
- Use school technologies at appropriate times, in approved places, for educational pursuits.
- Cite sources when using online sites and resources for research.
- Be cautious in the protection of the safety of my own safety and that of others.
- Help to protect the security of school resources.

Unacceptable Use - I will not:

- Use school technologies in a way that could be personally or physically harmful.
- Attempt to find inappropriate images or content. (The intent to seek inappropriate images or content is a violation of this Acceptable Use Policy.)
- Engage in cyber bullying, harassment, or disrespectful conduct toward others.
- Try to find ways to circumvent the school’s firewalls and filters. (The intent to circumvent safety measures is a violation of this Acceptable Use Policy.)
- Use school technologies to send spam or chain mail.
- Post or otherwise disclose personally-identifying information about myself or others.
- Use language online that would be unacceptable in the classroom.
- Use school technologies for illegal or inappropriate activities.
- Attempt to hack or access sites, servers, or content that is not intended for my use.

This is not an exhaustive list. All users must use their own good judgment when using school technologies.

Violations of the Acceptable Use Policy - Violations may have disciplinary consequences, including:

- Suspension of network, technology, or computer privileges;
- Employment disciplinary action.
- Legal action and/or prosecution.

I acknowledge the policy, the points identified in this declaration, and agree to follow and uphold the spirit and specific guidelines detailed.

Signed Date