| | |
|---|---|
| Version: | Final |
| Approved date: | October 2025 |
| Review date: | October 2026 |

# The British School of Gran Canaria

# **Online Safety Policy**

**Contents**



**APPENDICES**

## 1. Definitions

In this policy:

- **BSGC** – The British School of Gran Canaria (including both Tafira and South campuses).
- **Pupils / students / children** – all enrolments at the school.
- **School community** – pupils, staff, governors, and any users of our systems.
- **Governor** – member of the board with oversight responsibilities.
- **Senior Management Team (SMT)** – the school leadership team.
- **Head / Headteacher** – person with ultimate responsibility for school operations.
- **Online Safety Coordinator / Lead** – staff member responsible for implementing this policy.
- **Staff** – all school employees (teaching, administrative, technical, support).
- **Network Manager / ICT Technician** – staff responsible for ICT systems, filtering, security, access.
- **Data Manager / DPO** – the person or service responsible for data protection compliance.
- **AI / Synthetic media / Generative tools** – software that uses artificial intelligence to produce or alter audio, video, images, or text (e.g. deepfakes, chatbots, AI video generators).

## 2. Rationale & Purpose

At BSGC, we recognise that internet and digital technologies are central to students' learning, life, and future careers. But those same tools carry risks. This policy aims to:

- Define safe, responsible behaviours for using digital technologies and the internet.
- Provide protection for pupils, staff, and the school from online risks and abuse.
- Raise awareness across our community about threats, misuse, and responsible digital citizenship.
- Incorporate emerging technology issues (e.g. AI-generated media) into our safeguarding framework.
- Establish procedures for reporting, responding to, and recovering from online safety incidents.

## 3. Scope & Application

This policy covers:

- Use of school-owned and personally owned devices (laptops, tablets, phones) connecting to school systems or used for school purposes.
- Use of digital communication, cloud services, AI tools, social media, apps, and online platforms.
- Activities undertaken during or outside school hours that might relate to online safety or reflect on the school community.

While we cannot control all off-site digital behaviour, we commit to educating students and equipping them with strategies to stay safe online in all environments.

## 4. Roles & Responsibilities

**Governors / Online Safety Governor**

- Ensure this policy is current, reviewed annually, and fully implemented.
- Receive regular reports from the Online Safety Lead about incidents, trends, and policy compliance.
- Support resource allocation for training, monitoring, and infrastructure.

**Designated Safeguarding Lead and AI Lead**

- Oversee day-to-day implementation and review of this policy.
- Deliver staff training and awareness raising.
- Maintain an incident log, escalate serious issues, and analyse patterns.
- Liaise with ICT, pastoral, safeguarding leads, and governors.
- Monitor new technologies, risks, and update guidance accordingly.

**Headteacher**

- Ensure online safety is embedded in culture, curriculum, and practices.
- Collaborate with the Online Safety Lead and SMT to manage incidents, sanctions, and communications.
- Be aware of safeguarding risks arising from digital media, personal data misuse, grooming, cyberbullying, and synthetic media.

**Network Manager / ICT Technician**

- Manage filtering, firewall, device security, updates, monitoring.
- Assist staff with tools, access controls, and technical support.
- Log changes, filtering exceptions, and report to Senior Leadership as needed.

**Staff**

- Model responsible digital behaviour.
- Use AI/synthetic tools in class only with planning, supervision, and approval.
- Report concerns or misuse of digital media immediately to the Online Safety Lead or DSL.
- Uphold privacy, data protection, and consent guidelines when publishing or using images, video, or student work.

**Students**

- Use technology in line with the Acceptable Use Policy and this online safety policy.
- Report any discomfort, bullying, or misuse to a trusted adult immediately.
- Be taught how to use AI tools responsibly in school, critically evaluate content, and protect their digital identity.

**Parents / Carers**

- Support the school's online safety policy and acceptable use expectations.
- Work with the school to reinforce responsible technology use at home.
- Attend training or sessions provided about new digital/safeguarding matters (e.g. AI).

## 5. Digital Education & Curriculum Integration

We commit to integrating online safety and digital literacy into our curriculum:

- A structured online safety programme embedded in **Computer Science, PSHE, and cross-curricular lessons**.
- Regular assemblies and tutor-time sessions reinforcing key messages (reporting, fact-checking, consent).
- Explicit lessons or workshops on **AI, synthetic media, deepfakes, and misinformation** — students will learn how such media is created, how to spot manipulation, and the ethics involved.
- Critical thinking and verification skills taught across subjects (e.g. assessing sources, detecting deepfakes).
- Safe methods and scenarios for student use of AI tools in learning, with teacher oversight.

## 6. Staff Training & Awareness

- Annual required online safety training for all staff (including AI risks, synthetic media, new tools).
- Specific sessions during INSET on responsible use of AI, policy updates, incident handling.
- Ongoing updates, briefings, and shared resources to keep staff informed of emerging threats.

## 7. Technical & Infrastructure Safeguards

BSGC will maintain robust ICT safeguards to defend against misuse:

- Secure broadband, filtering, firewalls, anti-malware, intrusion detection.
- Regular audits and reviews of systems, filtering logs, access rights, and vulnerabilities.
- Devices, servers, and cabling secured physically and logins/passwords protected.
- Permissions and access rights defined per user roles; elevated rights limited.
- Procedures for controlled disabling of filters (only under supervision and logged).
- Users made aware that monitoring of network usage may occur.
- Requests for unblocking or changes must follow formal approval processes.
- Personal data transmission only via secure, encrypted channels.

## 8. Acceptable Use & Digital Conduct

All users must adhere to the Acceptable Use Policy (AUP). Key expectations:

**Permitted Use:**

- Use school technology for education, communication, research, and approved creative tasks.
- Cite sources and respect copyrights.
- Utilize AI tools responsibly when authorised and supervised.

**Unacceptable Use:**

- Accessing or distributing illegal content (e.g. indecent images, hate speech, piracy).

- Bypassing filtering or security measures.
- Creating or sharing AI-generated media depicting real individuals without consent, or used to mislead or harm.
- Cyberbullying, harassment, impersonation.
- Unauthorized disclosure of personal or confidential data.
- Using personal devices or accounts to conduct school-related digital work in violation of policy.

Violations may lead to disciplinary action, restrictions, or legal referral.

## 9. Incident Handling & Response

**Reporting and logging:**

- All online safety incidents (misuse, harassment, synthetic media concerns) must go into the online safety log and be reported to the DSL.
- Preserve the evidence (screenshots, URLs) without forwarding or altering content.

**Response:**

- DSL, Online Safety Lead, ICT, and Senior Leadership assess severity and risk.
- Follow child protection protocols if required, involving parents and external agencies (police) for serious incidents (e.g. deepfakes involving minors).
- Support the affected student(s) with pastoral care, counselling, and remediation.
- Review and refine policies or practices to prevent recurrence.

## 10. Legal Consequences under Spanish Law for AI / Synthetic Media Misuse

A legal context section summarising the legal consequences of misuse is set out in Appendix B, so that staff, students, and parents understand that misuse is not just against school policy, but may carry real legal risks and consequences (criminal, civil, and administrative).

The school will provide guidance and raise awareness with students, staff and parents about responsibilities and consequences in order to develop positive and responsible attitudes and use. (See Appendix C)

## 11. Mobile Device Initiative

All students' mobile devices that are brought into school for personal use are expected to have a parental control application installed. The school will monitor this compliance and remind parents of this expectation.

Students' mobile phones, and other technology that permits communication with third parties, will be collected at the beginning of the school day, stored centrally and retuned to students at the day. Non-compliance could mean the removal of the right to bring a phone, or other such device, into school.

## 12. Communication & Parental Engagement

- Online safety guidance, updates, and alerts will be published on the school website, newsletter, and via parent workshops.
- We will provide dedicated sessions on AI, synthetic media, safeguarding — available to parents, carers, and community.
- Encourage parental conversations at home about emerging technology, consent, and respectful media sharing.

## 13. Appendices & Supporting Documents

- **Appendix A**: AI-Generated Video Tools — Summary & Guidance
- **Appendix B**: Legal Consequences under Spanish Law for AI / Synthetic Media Misuse
- **Appendix C**: Strategies for Raising Awareness with Students
- **Appendix D**: Practical Classroom Guidance for Teachers (safe use of AI tools)
- **Appendix E**: Acceptable Use Agreements (Students, Staff, Parents)
- **Appendix F**: Incident report forms, escalation flowcharts
- **Appendix G**: Online Safety Incident Escalation Flowchart
- **Appendix H**: AI / Synthetic Media Incident Addendum

## 14. Policy Review & Updates

- This policy will be reviewed at least **annually**, or sooner if new technologies or risks emerge.
- Staff, governors, students, and parent feedback will inform updates.
- Any changes will be published, and training delivered to ensure awareness.

# Appendix A: AI-Generated Video Tools — Summary & Guidance

| Topic | Summary & Guidance |
|---|---|
| **What are AI-Generated Media Tools?** | AI video, image, and voice generation platforms (e.g., Sora, Runway, Pika Labs, Synthesia, DeepBrain, and D-ID) can create realistic content from text prompts or reference material, including people's likenesses and voices. |
| **Potential Misuse** | Misrepresentation ("deepfakes"), online harassment, reputational damage, misinformation, and creation of harmful or inappropriate content have been reported with many such platforms. |
| **Current Safeguards & Limitations** | While many tools include moderation filters, age restrictions, and content verification, they are not fail-safe. Misuse can still occur, especially through third-party or unregulated platforms. |
| **Risks to Children and Schools** | Emotional distress from manipulated media or impersonation- Erosion of trust in digital content- Exposure to inappropriate or sexualised AI content<br>Misuse in bullying or social exclusion- Overreliance on AI for learning or creativity |
| **What Schools Should Do** | Embed AI awareness into online safety education- Maintain clear policies on ethical use- Include AI in staff safeguarding training<br>Provide safe reporting routes for AI misuse- Liaise with parents to reinforce consistent expectations |
| **Parental Guidance** | Discuss with children how AI-generated content works and how it can be misleading- Encourage the question: *"Could this be AI?"* before sharing media<br>Set boundaries on use of AI tools at home- Model responsible and ethical engagement with technology |
| **When to Involve Authorities** | If AI-generated content involves minors in any indecent, threatening, or harassing form, it must be escalated immediately to **the police or relevant child protection agency**. This includes synthetic sexual images and impersonations. |
| **Reference Frameworks** | Guidance informed by the **Safe AI for Children Alliance**, **UK Safer Internet Centre**, and **NSPCC AI Safety Briefing (2025)**. |

# Appendix B - Legal Consequences under Spanish Law for AI / Synthetic Media Misuse

| Misuse / Scenario | Relevant Law / Article | Possible Legal Consequences |
|---|---|---|
| **Deepfake content with sexual, pornographic, or degrading material** | Proposed amendment to the **Spanish Penal Code, Article 173 bis** – criminalises the creation or dissemination of AI-generated sexual or seriously degrading deepfakes without consent. *(Source: merlin.obs.coe.int)* | • **Criminal offence** punishable by **imprisonment** (typically 1–4 years) and/or **fines**.<br>• **Permanent criminal record** and possible entry on the **Sex Offender Register**.<br>• **Civil liability** for moral and reputational damages to the victim.<br>• **Mandatory deletion** and removal orders for offending content. |
| **Dissemination of pornographic material to minors** | **Spanish Penal Code**, Title VIII (Crimes against Sexual Freedom), esp. **Articles 183–189**. 2024/25 reforms extend these to AI-generated or synthetic content. *(Source: La Moncloa)* | • **Serious criminal offence** with penalties of **2–6 years' imprisonment**.<br>• **Automatic referral** to law enforcement and child-protection authorities.<br>• **Prohibition from working with minors** or in education settings.<br>• **Confiscation** of involved digital devices and mandatory deletion of materials. |
| **Non-consensual use of someone's image or voice in manipulated media (identity misuse / harm to honour, dignity, image)** | **Spanish Constitution, Article 18** (right to honour, privacy, and image).**Organic Law 1/1982**, Articles 7–9 (civil protection of these rights). *(Source: LetsLaw)* | • **Civil lawsuit** possible by the affected person.- **Damages** for emotional distress or reputational harm (can exceed €30 000).<br>• **Court-ordered takedown** of offending material.<br>• **Potential criminal investigation** if defamation or harassment accompanies the misuse. |
| **Forgery / false identity or document manipulation** | **Spanish Penal Code**, **Articles 390–399 ter** and **Article 392** (forgery of public or private documents; identity fraud). *(Source: Ministerio de Justicia)* | • **Imprisonment** of **6 months to 3 years** for use of false identity or forged materials.<br>• **Increased penalties** if used to defraud, impersonate officials, or cause reputational harm.<br>• **Permanent record** and possible restriction on future travel or visa access. |
| **Violation of data protection / publication of images of minors without consent** | **GDPR**, esp. **Article 6.1** (lawful basis for processing).**LOPDGDD (Organic Law 3/2018)**, Articles 93–94 (digital rights and consent for minors aged under 14). *(Source: LetsLaw)* | • **Administrative sanctions** from the **Spanish Data Protection Agency (AEPD)** of up to **€20 million** or **4 % of turnover**.<br>• **Civil liability** for damages and reputational harm.- **Immediate removal orders** and compliance monitoring.- **Educational measures** or community service for minors involved. |
| **Failing to label AI-generated or synthetic content (transparency breach)** | **Draft Spanish AI Regulation Bill (2025)** aligning with the **EU AI Act**. Requires clear labelling of AI-generated audio, image, and video material. *(Source: Olive Press News Spain)* | • **Regulatory fine** up to **€35 million** or **7 % of global turnover** for serious infringements.- **Prohibition** on AI system use or publication.- **Mandatory rectification** (labelling, disclaimer, or takedown). |

# Appendix C - Strategies for Raising Awareness with Students

| Strategy | Description |
|---|---|
| **Curriculum Integration** | Lessons in PSHE / Digital Citizenship that include case studies of real legal cases (e.g. deepfake misuse), how the law treats synthetic media, etc. |
| **Workshops** | Special school workshops led by legal experts or digital safety specialists, focusing on consequences of AI misuse, privacy, consent. |
| **Assemblies / Tutor Time Sessions** | Short sessions to explain: what is AI / synthetic media; what is legal vs illegal; emphasize respect, consent, and honesty. |
| **Scenarios & Role-Play** | Run role-play scenarios where students consider: “If someone makes a deepfake of you without your consent, what consequences might there be legally and personally?” |
| **Student Contracts / Pledges** | Incorporate understanding of legal responsibilities into Acceptable Use Agreements or digital safety pledges. |
| **Parental Engagement** | Inform parents about legal issues; provide guidance so home supports school-led values and legal awareness. |
| **Visual Aids & Posters** | Infographics around school showing “Legal Risks of Misusing AI / Synthetic Media” with bullet points and what students should avoid. |
| **Monitoring & Reporting Mechanisms** | Encourage students to report misuse, with clear, safe and confidential routes; reinforce that misuse can have serious consequences. |

# Appendix D: Practical Classroom Guidance for Teachers — Safe Use of AI-Generated Tools

## 1. Purpose

This appendix provides clear, practical guidance for teachers and staff at The British School of Gran Canaria (BSGC) on the safe, ethical, and effective use of AI-generated video, image, and audio tools in educational settings.

It ensures that innovation enhances learning while maintaining the highest standards of safeguarding, privacy, and digital ethics.

## 2. Definition and Scope

"AI-generated tools" refer to platforms that use artificial intelligence to create or manipulate digital content — including, but not limited to:

- Video synthesis tools: Sora 2, Runway Gen-3, Pika Labs, HeyGen, Synthesia, DeepBrain, Veed.io, etc.
- Image generation tools: DALL-E, Midjourney, Leonardo AI, Adobe Firefly, Canva Magic Media.
- Audio and voice tools: ElevenLabs, PlayHT, Resemble AI, and similar.

This guidance applies to all staff, all year groups, and all BSGC devices or accounts.

## 3. Guiding Principles

1. **Safety First:** Student wellbeing and protection override all creative or instructional objectives.
2. **Transparency:** Always inform students when AI is used and discuss its limitations or ethical implications.
3. **Consent:** No student's image, likeness, or voice may be captured or replicated using AI tools without explicit consent from parents/carers and the student (where age-appropriate).
4. **Age-Appropriateness:** Only platforms that comply with GDPR and age restrictions may be used.
5. **Supervision:** All AI-related activities must be directly supervised by staff.
6. **Educational Purpose:** AI tools must only be used to enhance teaching and learning outcomes — never for entertainment or personal experimentation.

## 4. Approved Use in the Classroom

Staff may use AI tools to:

- Demonstrate concepts (e.g. visualising scientific processes, historical reconstructions, or creative storyboards).
- Support differentiated learning through accessible or multilingual resources.
- Encourage critical digital literacy, exploring how synthetic media is created and verified.
- Stimulate discussion around bias, truth, and responsible technology use.

All uses must be pre-planned, risk-assessed, and approved by the relevant Head of Department (HoD) or Digital Learning Lead.

## 5. Prohibited Use

Teachers and students must **not**:

- Generate or share AI content featuring real people (staff, students, or public figures) without informed consent.
- Create or display AI-generated content that could be misleading, offensive, discriminatory, or harmful.
- Use AI avatars, faces, or voices of minors in any synthetic media project.
- Upload student photos, names, or identifiers to third-party AI sites unless authorised by the school's data protection officer (DPO).
- Use personal AI accounts (non-school) for school activities.

## 6. Data Protection and GDPR Compliance

- All AI platforms must undergo data-privacy evaluation before classroom use.
- Any data shared with AI systems must be anonymised and minimised.
- Personal data must never be used to "train" AI tools.
- Staff should use official school accounts and store all generated content within approved school drives.
- Breaches or concerns must be immediately reported to the Head of Sector, DSL and DPO.

## 7. Teaching Digital Literacy

BSGC is committed to developing AI literacy as a key component of online safety education. Teachers are encouraged to:

- Help students identify AI-generated versus authentic media.
- Discuss real-world consequences of deepfakes and misinformation.
- Reinforce empathy, respect, and consent in digital creation.
- Use the school's motto — *Be Kind, Be Brave, Be You* — to frame responsible use and curiosity.

## 8. Staff Training and Support

The school provides:

- Regular INSET sessions on educational AI tools and safeguarding protocols.
- Updates from the AI Lead on emerging platforms and risks.
- Access to professional learning communities for sharing best practice.
- On-demand support for lesson planning, ethical dilemmas, and technical questions.

Staff are encouraged to seek advice from the AI Lead, ICT Coordinator, or DSL before introducing new AI tools.

## 9. Reporting and Escalation

If AI tools are misused, staff must:

1. Stop the activity immediately.
2. Preserve any evidence (screenshots, links).
3. **Inform the DSL and AI Lead without delay**.
4. Record the incident using the school's safeguarding reporting system (e.g. CPOMS).
5. Follow subsequent guidance or investigation procedures.

## 10. Review and Evaluation

This guidance will be reviewed annually, or sooner if major changes occur in AI regulation or technology.

Feedback from staff and students will inform updates to ensure that BSGC remains a safe, forward-thinking, and digitally responsible school.

## 11. Related Policies

- Child Protection & Safeguarding Policy
- Online Safety Policy
- Acceptable Use Policy (AUP)
- Data Protection & GDPR Policy
- Digital Learning Strategy

# Appendix E – 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

# Appendix F: Online Safety Incident Report Form (Template)

## The British School of Gran Canaria
## Online Safety / Digital Safeguarding Incident Report

| Section | Details |
|---|---|
| **Date & Time of Report:** | |
| **Reported By:** | Name, Role, Contact |
| **Date & Time of Incident (if known):** | |
| **Persons Involved:** | Pupil(s) / Staff / Parent / Other (list names, year groups, roles) |
| **Type of Incident (tick all that apply):** | ☐ Cyberbullying ☐ Inappropriate content ☐ Sexting / indecent image ☐ AI / Deepfake misuse ☐ Data breach ☐ Device misuse ☐ Online grooming ☐ Threat / intimidation ☐ Other (specify): _____ |
| **Brief Description of Incident:** | (Include what was seen / said / shared, by whom, and how it came to attention. Attach screenshots, URLs, etc. if relevant.) |
| **Immediate Actions Taken:** | (E.g., device confiscated, internet access restricted, DSL informed, parents contacted.) |
| **Who Has Been Informed:** | ☐ DSL ☐ Headteacher ☐ Online Safety Lead ☐ ICT Technician ☐ Parent/Carer ☐ Police / CEOP ☐ External Agency |
| **Initial Assessment of Risk:** | ☐ Low ☐ Moderate ☐ High (brief reasoning) |
| **Next Steps / Planned Follow-Up:** | (E.g., investigation, counselling, disciplinary, parental meeting, external referral) |
| **Completed By:** | Name / Signature / Date |
| **Reviewed By (DSL/Head):** | Name / Signature / Date |
| **Outcome / Closure Summary:** | (Actions completed, support provided, review date, lessons learned.) |

**Confidential:** This form should be stored securely in accordance with GDPR and school safeguarding record-keeping procedures.

# Appendix G: Online Safety Incident Escalation Flowchart

## 1. Identification

- Staff member, student, or parent identifies potential online safety concern or receives a report.
- DO NOT investigate independently beyond securing evidence (e.g., screenshots, URLs).

## 2. Report Immediately

- Report to the Designated Safeguarding Lead (DSL).
- If unavailable, contact the Headteacher or a Deputy DSL.
- Log initial details on the Incident Report Form.

## 3. Initial Assessment by DSL / Online Safety Lead

- Assess risk: *low*, *medium*, or *high*.
- Consider: Is anyone in immediate danger? Is this illegal? Does it involve synthetic or sexual content?
- Decide immediate protective actions (e.g., isolate device, remove content, contact parents).

## 4. Escalation Decision

| Risk Level | Example | Action / Escalation |
|---|---|---|
| **Low** | Mild inappropriate use, no harm, policy reminder needed | Record on log, inform tutor, follow-up with student. |
| **Moderate** | Repeated misuse, bullying, AI image manipulation, data leak | DSL investigation, parental meeting, possible disciplinary action. |
| **High / Illegal** | Child sexual imagery, grooming, threats, deepfake exploitation, hate speech | Contact Police / CEOP immediately. Inform Headteacher & Governors. Preserve evidence securely. |

## 5. Response & Support

- DSL coordinates safeguarding response.
- Pastoral and counselling support offered to affected students.
- Communication with parents (unless it increases risk).
- Disciplinary process applied where appropriate.
- Update Online Safety Log and record outcomes.

## 6. Review & Learning

- DSL/Online Safety Lead reviews incident for learning points.
- Update risk assessment, staff training, or policy where necessary.
- Report summary (anonymised) to governors in termly safeguarding review.

# Appendix H: AI / Synthetic Media Incident Addendum

When an incident involves **AI-generated content** (e.g., deepfake video, synthetic image, fake voice, or chatbot misuse):

1. Secure and preserve digital evidence (screenshots, links, metadata if possible).
2. Assess for potential illegality - if the content is sexualised, threatening, or defamatory, contact police immediately.
3. Do not share or forward the content - only preserve for safeguarding record.
4. Notify parents and affected individuals sensitively; explain what synthetic media is and steps being taken.
5. Provide education and support sessions for involved students to prevent recurrence.
6. Review filtering, monitoring, and teaching materials to include relevant AI literacy.