

Online Safety and Cyber Safety Policy

Aim

The aim of this policy is to keep students safe when using school technology, internet access, online platforms, devices, AI tools and digital communication. It promotes safe, respectful and responsible online behaviour, protects students from online harm, and supports the school safeguarding system.

Scope

This policy applies to all students, staff, parents/guardians, volunteers, visitors, contractors and any person using school devices, school accounts, school internet access, approved online platforms or digital communication linked to Brighton International Academy. It applies on school premises, during school activities, on school trips, during online learning and where online behaviour outside school affects student safety, wellbeing, learning or the reputation of the school.

Policy Statement

Brighton International Academy is committed to providing a safe digital learning environment. Online safety is part of child protection and safeguarding. Student safeguarding concerns must be recorded factually and reported immediately to Ms. Amany Al Sheikh, or to Ms. Eman Omar or another DDSL if she is unavailable. School-adult conduct concerns must follow Section 14 of the Child Protection and Safeguarding Policy. Staff must not investigate online safeguarding concerns themselves, promise confidentiality, delete evidence, forward harmful images or contact alleged perpetrators. Immediate safety, accurate recording and timely reporting are the priority.

Online Risks Covered

- Cyberbullying, harassment, threats, exclusion through group chats, online humiliation or repeated unkind digital communication.
- Unsafe contact, grooming, impersonation, pressure from unknown adults or requests for private information, photos, videos or meetings.
- Harmful content, including violent, sexual, extremist, self-harm, eating disorder, gambling, drug-related or age-inappropriate material.
- Image-based abuse, including sharing private images, taking photos without consent, edited images, fake images and deepfakes.
- AI misuse, including unsafe AI chatbots, fake content, deepfake media, automated bullying, plagiarism, misinformation and uploading identifiable student information.
- Data breaches, weak passwords, shared accounts, unauthorised access, phishing links, scams, malware or misuse of school accounts.
- Harmful online challenges, livestream risks, excessive screen use, age-restricted platforms and online behaviour that affects school safety or wellbeing.

Roles and Responsibilities

- School Leadership: ensures online safety systems, staff training, supervision, accountability and policy implementation are in place.
- DSL - Ms. Eman Omar: has overall safeguarding oversight of online safety concerns, records, risk decisions, parent communication and referrals where needed.
- DDSLs - Ms. Rubita Tahir, Ms. Ouassila Abbi, Ms. Amany Elshikh and Ms. Susan Oommen: support the DSL

Vision: To foster academic excellence, nurture ethical values, and develop leadership skills, preparing students to thrive in a diverse world.

Mission: We promote intellectual growth, ethical responsibility, and global awareness, empowering students to contribute positively to society.

Motto: Rooted in faith, striving for excellence

with student follow-up, concern review, recording and safety actions.

- ICT/IT Team: maintains filtering, monitoring, approved platforms, accounts, devices and technical evidence when authorised by school leadership/DSL.
- Teachers and Staff: supervise technology use, model safe behaviour, protect student data, teach safe use and report concerns promptly.
- Students: use technology respectfully, keep passwords private, report concerns, and do not record, share or post content that could harm others.
- Parents/Guardians: support safe device use at home, monitor age-appropriate access, report concerns early and work with the school to keep children safe.
- Visitors, Volunteers and Contractors: use school systems only when authorised and must follow safeguarding, confidentiality, photography and reporting expectations.

Acceptable Use, Accounts and Password Safety

1. School technology, accounts, internet access and platforms must be used for authorised learning and professional purposes only.
2. Students, parents/guardians and staff must complete the relevant Acceptable Use Agreement before access to school systems or devices is granted. Student acknowledgement must be supported in an age-appropriate way.
3. School accounts must not be shared. Passwords must be private, secure and changed when a risk is suspected.
4. Staff must not allow students to use staff accounts, staff devices or unlocked screens.
5. Unauthorised software, apps, VPNs, proxy sites, external storage must not be used on school systems without approval.
6. Any suspected account breach, phishing message, inappropriate access or data loss must be reported immediately to ICT/IT and the DSL/DDSL where student safety or data is involved.

Filtering, Monitoring and Technical Controls

1. Filtering and monitoring systems are used to block unsuitable content and identify possible online safety risks.
2. The ICT/IT Team will maintain appropriate access controls, approved platforms, device settings and monitoring records.
3. Repeated blocked searches, attempts to bypass filters, access to harmful content or unusual account activity must be reviewed and reported where needed.
4. Technical evidence may be preserved only by authorised staff. Staff must not search students' devices or accounts unless this is permitted through school procedures and authorised by leadership/DSL.
5. Filtering and monitoring evidence will be reviewed at least termly by the DSL, supported by the DDSLs, ICT/IT and the safeguarding committee.

AI Tools, Chatbots, Deepfakes and Digital Content

1. AI tools may be used only for approved educational or professional purposes and must be supervised appropriately.
2. Staff must not upload identifiable student information, safeguarding records, assessment data, images or confidential school information into AI tools unless the tool has been approved by the school for that purpose.
3. AI tools must not be used to make safeguarding, behaviour, disciplinary, admissions, assessment or risk decisions about students.

Vision: To foster academic excellence, nurture ethical values, and develop leadership skills, preparing students to thrive in a diverse world.

Mission: We promote intellectual growth, ethical responsibility, and global awareness, empowering students to contribute positively to society.

Motto: Rooted in faith, striving for excellence

4. Students must be taught that AI content may be inaccurate, biased or unsafe and that they must not use AI to bully, impersonate, create fake images, deepfakes or misleading content.
5. Any deepfake, fake image, sexualised image, impersonation, AI-generated abuse or harmful AI chatbot concern must be treated as an online safeguarding concern and reported immediately.

Mobile Devices, Images, Video and Social Media

1. Student mobile phone use must follow the school mobile phone and behaviour procedures. Unauthorised use, filming, photographing, recording or sharing content is not allowed.
2. Students must not take, edit, share or post images, videos or voice recordings of others without permission and school approval.
3. Staff must use school-approved devices, accounts and platforms for school communication and must not contact students through personal social media or private messaging.
4. Staff must not store student images or videos on personal devices. Any accidental capture, sharing error or media concern must be reported promptly.
6. Cyberbullying, humiliation, threats, group-chat targeting, image sharing, fake accounts or harmful social media posts linked to school must be recorded and reported.

Reporting and Response Procedure

1. Listen, reassure and take the concern seriously. Thank the student or adult for reporting.
2. Check immediate safety. Separate students or secure supervision where needed.
3. Do not investigate, question widely, delete evidence, forward harmful images or ask students to show distressing material unnecessarily.
4. Record the concern factually, including the student's or informant's own words, date, time, platform, people involved, location of existing evidence and immediate action taken. Do not create screenshots, copies or downloads of harmful images. Evidence handling must follow authorised safeguarding procedures.
5. Report student safeguarding concerns immediately through Section 10.2 of the Child Protection and Safeguarding Policy. Allegations or concerns about school-adult conduct must follow Section 14.
6. Inform ICT/IT where technical action is needed, such as securing an account, preserving evidence, checking filtering logs or blocking access.
7. Safeguarding parent/carer communication must be managed by the DSL/DDSL under Section 12 of the Child Protection and Safeguarding Policy. Parents must not be contacted where this could increase risk or compromise safeguarding action.
8. Agree and record follow-up actions, including student support, behaviour response, parent communication, technical action, monitoring and referral where required.

Education, Prevention and Parent Partnership

- Students are taught online safety through ICT, PSHE/SEL, assemblies, class reminders, homeroom discussions and age-appropriate awareness activities.
- Teaching will include safe communication, trusted adults, cyberbullying, privacy, passwords, age restrictions, online grooming, AI risks, deepfakes, harmful content and respectful online conduct.
- Parents/guardians will receive online safety reminders and may be offered guidance on age-appropriate apps, screen time, parental controls, reporting and responding to cyberbullying.
- The school will use student voice, posters, assemblies and wellbeing activities to encourage students to report concerns early and seek help from trusted adults.

Record Keeping and Confidentiality

- Online safety concerns must be recorded accurately, securely and in line with the Child Protection and Safeguarding Policy, Behaviour Policy, Anti-Bullying Policy and Data Protection procedures.
- Records should include dates, times, platform/device, students involved, what was seen or reported, immediate actions, parent contact, evidence location and follow-up review.
- Sensitive evidence must be handled carefully and only shared with staff who need to know. Harmful images must not be printed, copied, forwarded or stored on personal devices.
- Where a data breach is suspected, the school data/confidentiality procedures must be followed alongside safeguarding reporting where student safety is involved.

Monitoring and Evaluation

Online safety will be monitored through training records, Acceptable Use Agreement trackers, filtering and monitoring logs, incident records, student voice, parent communication, curriculum evidence, safeguarding records and ICT/IT review. The DSL, supported by the DDSLs, will review online safety evidence with ICT/IT and the safeguarding committee at least termly. Patterns will be used to improve supervision, technical controls, PSHE/SEL teaching, parent communication and staff training.

Policy Management and Review

Policy Created By:	Ms. Nabilah Elharraj
Reviewed by:	Ms. Eman Omar
Reviewed on:	April 2026
Next Review Date:	April 2027
Review Cycle:	Annual
Approval Authority:	Ms. Eman Omar

Vision: To foster academic excellence, nurture ethical values, and develop leadership skills, preparing students to thrive in a diverse world.

Mission: We promote intellectual growth, ethical responsibility, and global awareness, empowering students to contribute positively to society.

Motto: Rooted in faith, striving for excellence