British International Remote School (BIRS)
Online Safety Policy

Effective Date:

1. Purpose

This policy aims to ensure that all students and staff at BIRS use online technologies safely, responsibly, and respectfully. It works in conjunction with our **Safeguarding and Child Protection Policy** and **Acceptable Use Policy (AUP)**. The term "online safety" encompasses internet safety and other risks associated with digital technologies.

2. Scope

This policy applies to all members of the BIRS community (staff, students, volunteers, contractors) when using school-provided or school-related digital technologies, platforms, and communication tools, whether on school-owned devices or personal devices used for BIRS educational purposes.

3. Key Online Safety Principles

3.1. **Education:** BIRS will integrate age-appropriate online safety education into its curriculum, covering topics such as responsible online behaviour, privacy, critical evaluation of online content, and recognizing online risks.

3.2. **Safe Practices:** BIRS promotes the following safe practices:

a) **Passwords & Security:** Students and staff must use strong, unique passwords for all BIRS accounts and keep them private. Multi-factor authentication will be encouraged/used where available.

b) **Personal Information:** Exercise caution when sharing personal information online. Understand what constitutes personal information and the risks of oversharing.

c) **Risk Awareness:** Understand and be able to identify risks such as cyberbullying, online grooming, sexting, exposure to inappropriate or harmful content (e.g., extremist, violent, pornographic), and online scams.

d) **Critical Evaluation:** Critically evaluate online information for accuracy, bias, and reliability.

e) **Secure Learning Environment:** Ensure learning environments (both for staff teaching and students learning) are free from inappropriate background visuals or sounds. Webcams should be used appropriately, with consideration for privacy (e.g., using virtual backgrounds or ensuring neutral backgrounds, avoiding private spaces like bedrooms where possible for teaching).

f) **Digital Footprint & Reputation:** Understand the permanence of online actions and the importance of maintaining a positive digital footprint.

g) **Copyright & Plagiarism:** Respect copyright, intellectual property rights, and academic integrity online.

3.3. **Reporting:** Clear, accessible procedures will be in place for students, staff, and parents to report any online safety concerns (e.g., cyberbullying, unwelcome contact, harmful content, security breaches) immediately to the Designated Safeguarding Lead (DSL) or other designated staff members. All reports will be taken seriously and investigated appropriately.

3.4. **Technical Measures:** BIRS will implement appropriate technical measures, such as robust security settings on school platforms, using vetted educational tools with strong privacy features, and applying filtering on BIRS-managed networks where technically feasible and appropriate for our learning environment, to enhance online safety.

3.5. **Professional Communication:** All online communication between staff and students must take place via official BIRS channels and must maintain professional boundaries at all times, as outlined in the **Staff Code of Conduct** and **AUP**.

4. Responsibilities

4.1. BIRS (Leadership & Management):

a) To provide and maintain a safe online learning environment.
b) To ensure this policy is implemented, communicated, and regularly reviewed.
c) To provide appropriate online safety education and training for students and staff.
d) To ensure clear and effective reporting and response mechanisms are in place.

4.2. **Staff (Teaching and Non-Teaching):**

a) To read, understand, and adhere to this Online Safety Policy, **the AUP**, and the **Staff Code of Conduct**.
b) To model safe, responsible, and professional online behaviour.
c) To integrate online safety education within their teaching where appropriate.
d) To be vigilant for online safety risks and follow reporting procedures promptly.
e) To manage online classroom environments safely.

4.3. **Students:**

a) To act responsibly and respectfully online, adhering to this policy and **the AUP**.
b) To protect their personal information and respect the privacy of others.
c) To report any online safety concerns or incidents to a trusted adult staff member immediately.
d) Not to engage in, encourage, or condone cyberbullying or any form of online harm.

4.4. **Parents/Guardians:**

a) To read and support this Online Safety Policy and discuss online safety with their child.
b) To encourage their child to use online technologies responsibly and safely.
c) To monitor their child's online activity at home as appropriate for their age and maturity.
d) To report any online safety concerns related to BIRS or its community to the school.

5. **Responding to Online Safety Incidents:**

BIRS will respond to online safety incidents promptly and appropriately, in line with its **Safeguarding and Child Protection Policy**, disciplinary procedures, and relevant legal requirements. Responses may include:

a) Investigation of the incident.
b) Providing support to any students or staff affected.
c) Taking disciplinary action against those responsible, where appropriate.
d) Removing inappropriate content from BIRS platforms where possible.
e) Liaison with parents/guardians.
f) Referral to external agencies (e.g., child protection services, police, CEOP) if necessary.
g) Reviewing practices to prevent future incidents.

6. **Review**

This Online Safety Policy will be reviewed at least annually by the DSL and senior leadership, in conjunction with the **Safeguarding and Child Protection Policy**, or sooner if required by new legislation, guidance, or emerging online risks.