

Online Safety Policy

Policy Title			Online Safety Policy								
Policy Owner			Head of Technology								
Approval Body			Works Council / Management Board / Supervisory Board								
Date Reviewed & Approved			February 2025								
Policy review date			February 2026								
Statutory policy	Yes	No	On website	Yes	No	On parent portal	Yes	No	On staff portal	Yes	No

Contents

1. Aims	2
2. Legislation and guidance (required)	3
3. Definitions and scope (required)	3
4. Roles and Responsibilities	3
4.1 The Leadership and Management Team.....	3
4.2 The Designated Safeguarding Lead (DSL).....	3
4.3 Staff Responsibilities.....	4
4.4 Technical Staff Responsibilities.....	4
4.5 Learners and Parents.....	4
5. Education and Engagement Approaches	4
5.1 Education with Learners.....	4
5.2 Training with Staff.....	4
6. Reducing Online Risks	5
7. Safer Use of Technology	6
7.1 Classroom Use.....	6
7.2 Filtering and Monitoring.....	6
7.3 Data and Security.....	6
7.4 Managing Email and Learning Platforms.....	6
8. Social Media	6
8.1 Expectations.....	6
8.2 Staff Personal Use.....	6
8.3 Official Use of Social Media.....	7
9. Use of Personal Devices and Mobile Phones	7
9.1 Expectations.....	7
9.2 Staff Use.....	7
9.3 Learners' Use.....	7
10. Responding to Online Safety Incidents and Concerns	7
10.1 Reporting Procedures.....	7
10.2 Specific Incidents.....	8
11. Monitoring Arrangements	8

1. Aims

The purpose of The British School of Amsterdam’s online safety policy is to:

- Safeguard and protect all members of The British School of Amsterdam’s community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

The British School of Amsterdam believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online. We

believe that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.

2. Legislation and guidance

This online safety policy takes account of the DfE statutory guidance Keeping Children Safe in Education and relevant safeguarding procedures.

As an accredited British School Overseas, this document meets the requirements set out in the Standards for British Schools Overseas. In case of discrepancies, local law or regulations will take precedence

This policy complies with GDPR regulations, as arranged in the AVG framework and with the Wet Veiligheid op school, which sets out schools' obligations to keep children safe (online).

3. Definitions and scope

Online safety risks are diverse and evolving. The British School of Amsterdam addresses the breadth of these challenges by organising them into four strategic risk areas, ensuring targeted depth in our prevention and response protocols:

- Content: Being exposed to illegal, inappropriate or harmful material.
- Contact: Being subjected to harmful online interaction with other users.
- Conduct: Personal online behaviour that increases the likelihood of, or causes, harm.
- Commerce: Risks such as online gambling, inappropriate advertising, phishing or financial scams.

Scope of Policy This policy applies to all staff, Supervisory Board members, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as learners, parents and carers.

This policy applies to This version connects the policy to the **School Network** or the **School Equipment**, regardless of where the person is standing.

This policy applies to all access to the internet and use of technology when:

- Using **School-issued devices** (e.g., laptops, tablets, phones), regardless of location or network;
- Accessing the **School network or systems** (e.g., via VPN or school Wi-Fi) using personal devices;
- Performing **official school duties** or representing the school in an online capacity.

4. Roles and Responsibilities

4.1 The Leadership Teams

The Leadership Team will:

- Online safety is managed as a fundamental part of the school's safeguarding culture. The school ensures that its digital safety protocols align with UK best practices (such as KCSIE) while strictly adhering to local Dutch legal requirements and reporting mandates (the Meldcode). Where local and

national recommendations differ, the school will adopt the practice that provides the most robust protection for the child.

- Ensure there are appropriate and up-to-date policies regarding online safety, including a staff code of conduct and acceptable use agreement.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Ensure that all members of staff receive regular, updated, and appropriate online safety training.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns.

4.2 The Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead (DSL), **Mrs H Rigelsford**, has lead responsibility for online safety. Mrs H Rigelsford will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies.
- Liaise with staff (especially Pastoral Support Staff, school First Aiders, IT Technicians and Heads of Learning Support) on matters of safeguarding that include online and digital safety.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the Principal, Management Board or Supervisory Board..

4.3 Staff Responsibilities

It is the responsibility of all members of staff to:

- Read and adhere to the online safety policy and acceptable use policies.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Identify online safety concerns and take appropriate action by following the safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support.

4.4 Technical Staff Responsibilities

Staff managing the technical environment will:

- Implement appropriate security measures (e.g., password protected devices with encryption) to ensure that the IT infrastructure is secure.
- Ensure that the filtering policy is applied and updated on a regular basis.
- Report any filtering breaches to the DSL and Management Board.

4.5 Learners and Parents

- Learners: Are responsible for keeping themselves and others safe online, reading and adhering to the Acceptable Use Agreement, and seeking help from a trusted adult if there is a concern.
- Parents: Are responsible for reading acceptable use policies, supporting the school's approach by discussing online safety with their children, and identifying changes in behaviour that could indicate risk.

5. Education and Engagement Approaches

5.1 Education with Learners

The School Leadership teams will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible online behaviour by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in PSHE, RSE and computing programmes of study.
- Educating learners in the effective use of the internet to research, including skills of knowledge location, retrieval and evaluation.

5.2 Training with Staff

The school will provide and discuss the online safety policy with all members of staff as part of induction and provide up-to-date training at least annually.

7. Safer Use of Technology

All technology use at BSA is governed by the **Acceptable Use Policy (AUP)**. Use of school systems constitutes agreement to these terms:

- **Classroom & Supervision:** Staff must vet all school based digital tools/apps before use. Students will be supervised appropriately according to their age and ability.
- **Filtering & Monitoring:** The school utilizes Fortinet and Securly to block illegal, extremist, or inappropriate content (including the IWF list). All network traffic is monitored; safeguarding alerts are escalated directly to the DSL per the Child Protection Policy.
- **Security & Data:** Users are responsible for password confidentiality. Systems are protected by encryption and antivirus measures. Personal data is handled strictly in line with Data Protection legislation.
- **Official Channels:** Staff must use school-issued email and Google Workspace accounts for all professional business. Use of personal email for school duties is prohibited.

8. Social Media

8.1 Expectations

- The term social media includes blogs, wikis, social networking sites, forums, and chatrooms.
- All members of The British School of Amsterdam community are expected to engage in social media in a positive, safe and responsible manner.

8.2 Staff Personal Use

- Staff are advised that their online conduct on social media can have an impact on their role and reputation.
- Staff are strictly prohibited from connecting with current learners on any social media platform, including LinkedIn.

Regarding **past learners (Alumni)**, staff may connect on **professional networking sites (specifically LinkedIn)** only provided that:

- The learner has permanently left the school;
- The learner is at least 18 years of age;
- The connection is for the sole purpose of professional networking, references, or career guidance;
- The staff member ensures that the communication remains formal and professional at all times.

8.3 Official Use of Social Media

- The British School of Amsterdam's official social media channels (e.g., Facebook and Instagram, LinkedIn) are for clear educational or community engagement objectives .
- Official use is approved by the School.
- Staff must not engage in private messaging with learners or parents via official channels.

9. Use of Personal Devices and Mobile Phones

9.1 Expectations for students

- The British School of Amsterdam has a clear policy on mobile phone devices: **Never used, seen or heard.**
- Pupils may possess phones only if they are switched off and remain in school bags throughout the school day.
- The school accepts no responsibility for loss, theft, or damage of personal devices.

9.2 Staff Use

- Staff will ensure personal device use follows confidentiality and child protection policies.
- Staff must keep phones on silent during lesson times and not use them during teaching periods unless for Multi factor Authentication for Google and CPOMS.
- Staff are not permitted to use personal phones to contact pupils or parents.
- Staff will not use personal devices to take photos or videos of learners.

9.3 Learners' Use

- If a learner breaches the policy, the phone will be confiscated and held in a secure place.
- Searches of mobile phones will only be carried out in accordance with government guidance.
- If illegal material is suspected, the device will be confiscated and the police contacted.

10. Responding to Online Safety Incidents and Concerns

10.1 Reporting Procedures

- All members of the community must report concerns including breaches of filtering, youth produced sexual imagery, cyberbullying, and illegal content.
- Safeguarding provisions and policies fully apply to online activity and presence.

10.2 Specific Incidents

- **Online Sexual Violence/Harassment:** We will immediately notify the DSL and act in accordance with child protection policies. We will provide necessary safeguards and support for learners involved.

- **Youth Produced Sexual Imagery ('Nudes'):** This is a safeguarding issue. We will not view images unless necessary for safeguarding, nor will we copy/share them. We will act in accordance with child protection policies.
- **Online Radicalisation:** If we are concerned that a child or staff member is at risk of radicalisation online, the DSL or Principal will be informed immediately.

11. Monitoring Arrangements

The Head of Technology will monitor the effectiveness of this policy. This policy will be reviewed by the Head of Technology at least annually. At each review, the policy will be approved by the Management Board