BRITISH INTERNATIONAL SCHOOL

E-Safety policy

The British International School, Belgrade (BIS) is committed to safeguarding and promoting the welfare of children and expects all staff and volunteers to share this commitment.

Reviewed: June 2026

Review date: June 2027

Contents

Policy statement 3
Aims 3
Terminology 3
Scope 3
Responsibilities 3
Heads of School 4
Online Safety Team 4
IT Manager and IT Technical Support 4
E-Safety Lead 5
All staff 5
All Students 5
Parents and Carers 6
Procedure 6
Technology 6
Safe Use 7
Filtering and Monitoring 8
Settings and Notifications 8
Roles and Responsibilities 9
Incidents 10
Record keeping 11
Training 11
Curriculum 11
Cyber-bullying 13
Preventing and addressing cyber-bullying 13
Examining electronic devices 13
How the school will respond to issues of misuse 13
Remote learning 14

Policy statement

At the British International School, we use technology and the internet extensively across all areas of the curriculum. Although the advantages are clear, technology brings with it new and evolving risks, which need to be identified, assessed and mitigated where possible. Online safety, also referred to as e-safety, is an area of safeguarding that is having to adapt frequently and constantly, and as such **this policy will be reviewed on an annual basis or in response to an online incident, whichever is sooner.**

This policy is available for anybody to read on the BIS website. A copy of the *E- Safety Policy* will be made available on the parental portal. Terms and conditions of this policy are that the students will have permitted access to school technology including the internet.

Aims

Our school aims to:

- have robust processes in place to ensure the online safety of pupils, staff and volunteers;
- deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology;
- establish clear mechanisms to identify, intervene and address incidents appropriately.

Terminology

For clarity, the E-Safety Policy uses the following terms unless otherwise stated:

Users – refers to staff, school volunteers, students and any other person working in or on behalf of the school, including contractors

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer

School Community – students, all staff, parents

DSL – Designated Safeguarding Lead

SLT – Senior Leadership Team

IT or ICT – Information Technology or Information Communication Technology

BYOD – Bring your own device

Scope

The expectations identified in this policy apply to all members of the school community.

Responsibilities

The following responsibilities identified below are delegated to ensure thorough policy governance.

Heads of School

Reporting to the School Proprietor, the Heads of School have overall responsibility for e-safety within our school in conjunction with the DSL. The day-to-day management of this will be delegated to the E-Safety Lead as indicated below.

The Heads of School will ensure that:

- e-safety training throughout the school is planned and up to date and appropriate to the recipients
- the designated E-Safety Lead have had appropriate CPD in order to undertake the day-to-day duties;
- all online safety incidents are dealt with promptly and appropriately.

Online Safety Team

The Online Safety Team includes: the E-Safety Lead, DSL and the Safeguarding Team, and IT Manager.

The Online Safety Team will:

- keep up to date with the latest risks to children whilst using technology;
- familiarise him/herself with the latest research and available resources to support safe use of technology at school and at home;
- advise the Heads of School and Senior Leadership Team on all online safety matters;
- ensure all staff are suitably trained in relevant online safety issues;
- engage with parents and the wider school community on online safety matters at school and/or at home;
- retain responsibility for reporting and recording online safety incidents;
- ensure that the school community knows how to report an online safety incident
- ensure that there is an appropriate audit trail when an online safety incident is reported;
- ensure any technical online safety measures in school (e.g. internet filtering software and tools) are fit for purpose through liaison with IT Support and other agencies;
- ensure that all filtering and monitoring procedures are effectively implemented and regularly evaluated by the E-Safety Lead and IT Manager;
- ensure that relevant staff are suitably trained the use of the filtering and monitoring software where appropriate;
- oversee the online safety curriculum and ensure that its coverage is thorough, age-appropriate, up-to-date and relevant;
- lead in the planning of the annual Safer Internet Day;
- review this policy regularly and bring any matters to the attention of the Heads of School or a member of SLT.

IT Manager and IT Technical Support

The Head of IT is responsible for ensuring that the IT technical infrastructure is secure; this will include at a minimum:

- anti-virus is fit-for-purpose, up to date and applied to all capable devices;
- operating system updates are regularly monitored, and devices updated as appropriate;

- any online safety technical solutions, such as internet filtering, are operating correctly and in accordance with any GDPR regulations or legislation;
- filtering levels/settings are applied appropriately;
- passwords are applied correctly to all users regardless of age;
- passwords for staff will be a minimum of 8 characters.
- all account passwords, including the IT System Administrator password, are to be changed every 45 days, or earlier if a password's security is suspected of being compromised in any way;

E-Safety Lead

In addition to the IT Manager, the E-Safety Lead has a leading role in internet security at our school. In a way, the role of this position is partly from the IT department, and belongs to the Safeguarding team and protocols.

- must have adequate Safeguarding and especially E-safety training
- must have sufficient IT skills to be able to work with programs and applications that are in use
- have to be a trustworthy person and bear the responsibility that, together with the DSL, can recognize the threat, react quickly and help the vulnerable category
- Must know the process of filtering and monitoring and perform day to day activities
- Must prepare written evidence as a weekly and, if necessary, more frequent report

All staff

All staff, including contracted staff and volunteers who use technology in school, are to ensure that:

- all details within this policy are understood. If anything is not understood it should be brought to the attention of a member of the Online Safety Team
- any online safety incident is reported to a member of the Online Safety Team
- any online safety concerns where our existing systems fail to protect and fall short of expectations, e.g. viruses, spam and other breaches of security, must be reported immediately to IT Manager
- concerns involving a member of staff's inappropriate use of technology should be reported to a Head of School (*Safeguarding & Child Protection Policy* or *Whistleblowing Policy*);

All Students

The boundaries of use of ICT equipment and services in this school are given in the *Students' Acceptable Use Policy*; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the *Behaviour Policy*.

Online safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly, all students will be made aware how they can report areas of concern whilst at school or outside of school (concern will be raised and handled in accordance to our Safeguarding Policy).

Parents and Carers

Parents play the most important role in the development of their children; as such the school will offer current information, support and training to parents relating to online safety matters where appropriate, helping them with the skills and knowledge they need to ensure the safety of children outside the school environment. Through parent workshops and school newsletters, the school will keep parents up to date with new and emerging online safety risks and will involve parents in strategies to ensure that students are empowered.

Parents should understand that the school needs to have rules in place to ensure that their child can be properly safeguarded. Parents are asked to notify a member of staff of any school-related online safety concerns they may have or queries regarding this policy.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- UK Safer Internet Centre
- Childnet International
- Childnet International

Procedure

Technology

BIS uses a following of devices, including PCs and laptops. In order to safeguard students and in order to prevent loss of personal data, we employ the following assistive technology:

Internet Filtering – we use the product DNS Filter to restrict access to any inappropriate content on all devices connected to the campus network. BIS also uses NettSupport DNA as a filtering and monitoring tool for all student activity whilst they are logged into their BIS online accounts. For further information regarding filtering and monitoring, see 'Filtering and Monitoring' section below.

Monitoring - All staff, students and parents of students will be informed that internet activity and emails may be monitored in order to ensure, as much as possible, that users are not exposed to, or seek to access, illegal or inappropriate websites. Whilst using their BIS online accounts, student activity can be monitored using the web tool NettSupport DNA. The importance of monitoring, how and why the process is carried out, is openly discussed with staff and students at least once a year. A cover note will also accompany the *Students' Acceptable Use Policy*, openly inviting any questions regarding the matter. For further information regarding filtering and monitoring, see 'Filtering and Monitoring' section below.

Passwords – all staff and students that have school account will be unable to access their personal school account without a unique username and password. Staff and student passwords will change every 45 days or if there has been a compromise, whichever is sooner. The IT Manager is responsible for ensuring that passwords are changed.

Some devices in school do have shared access, such as computers in Primary school. Nevertheless, all staff and students are required to log in to their school server account or BIS online account in order to store their work. All staff and students must also ensure that they log out of their accounts when finished.

Anti-Virus – all capable devices will have anti-virus software. This software will be updated under

Microsoft policy for new virus definitions. The IT Manager will be responsible for ensuring this task is carried out and will report to the Heads of School if there are any concerns. All peripherals such as USB key-drives are to be scanned by Microsoft automatically for viruses before use.

Onboarding – BIS operates an onboarding style network. Onboarding is the process by which a new device gains access to the wired or wireless network for the first time. The onboarding system has been introduced to:

- improve network security;
- improve network performance;
- reduce the IT department workload relating to network access;
- allow users to connect quickly and securely to our network services.

School provided devices will be registered automatically with the network before being issued to students and staff. Software updates for all devices should be maintained to prevent any network connection disruption.

Safe Use

Internet – use of the internet in school is a privilege, not a right. Internet use will be granted to staff upon their acknowledgment and agreement to the terms of the *Staff Acceptable Use Policy*. Internet use will be granted to students once they have agreed to the terms of the relevant *Student Acceptable Use Policy*.

Email – all staff are reminded that emails are subject to *freedom of information* requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature should be avoided using the school account. Students have their own BIS online account (Google) and as such will be given their own email address. The email addresses are activated when the students enrol with a personal password which they are asked to change immediately and not disclose to anyone else.

Photos and videos – In Primary school parental permission to take photographs and videos of students is requested each year within the annual registration files. In Secondary school parental permission is requested only upon enrolment and can be altered on parents request at any time.

Any images or videos taken for school use should be uploaded, sent or transferred to the relevant school system (school social media account or school newsletters) as soon as possible and then deleted from the device.

When taking photographs and videos for school purposes we:

- do not identify a student by name when his or her image appears on the school website or on social media, unless specific permission has been granted by the parents/carers;
- ensure pupils and staff are appropriately dressed;
- ensure pupils are undertaking an official BIS activity only

We will follow the General Data Protection Regulation when taking and storing photos and recordings for use in the school.

Staff will not take photographs or videos of pupils on their personal phones or cameras. Staff will be provided with suitable devices to take pictures and recordings.

Social Networking – there are many social networking services available; the BIS is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community.

Should staff wish to use other social media, permission must first be sought via a member of the Online Safety Team who will advise the Heads of School for a decision to be made. Any new service will be risk assessed before use is permitted.

In addition, the following is to be strictly adhered to:

- images and videos of children must not be used if parents have indicated this in their registration files;
- there is to be no identification of students using first name and surname; first name only is to be used;

Other online services are also used to share curriculum content and allow students to interact and contribute to online discussions and collaborative learning tasks, therefore opening opportunity for two-way communication. These include services such as Google Classroom.

Safe Searching – students will be required to use search engines frequently to support their learning throughout the school. Although internet searching is a very powerful and beneficial skill for students to learn, the school also understands that this is an activity whereby the risk that children may be exposed to offensive content is increased, due to the open- ended nature of the process.
Nevertheless, the quality of the search results can be limited when using search engines which are not as powerful as tools, such as Google. Therefore, students are taught how to search safely and how to respond suitably when exposed to inappropriate or offensive content.

Filtering and Monitoring

An effective **filtering** system needs to block internet access to harmful sites and inappropriate content. An effective filtering system should not unreasonably impact teaching, learning and school administration, nor should it restrict students from learning how to access or manage risk themselves.

Monitoring user activity on school devices is an important part of providing a safe environment for students and staff. For monitoring to be effective, it should identify concerns promptly, usually through alerts or observations, allowing staff to take effective action and record the outcome.

Settings and Notifications

DNS Filter uses a technology that helps manage and control internet access by filtering and blocking unwanted or malicious content at the Domain Name System (DNS) level. It works by redirecting users' web requests through a filtering system that checks the requested domain names against a database of categorised websites. DNS Filter works on all devices which connect to the school's internet, through ethernet or wirelessly.

NettSupport DNA also filters and blocks unwanted or malicious content, and works when students are logged into their BIS online accounts. Automated reports are generated regularly, listing when users attempt to visit 'blocked' sites, intentionally or unintentionally. These blocked sites fall under categories, such as drugs, gambling, pornography, hate, etc. If a blocked website activity indicates concerns about a student's safety or well-being, the matter will be referred to the Safeguarding Team. (e.g. DSL and ADSLs).

Furthermore, NettSupport DNA monitors student activity and alerts designated staff at several levels:

- can track exactly the user's statement
- can select by disturbing key words

- can trace the source
- can automatically assign a category and provide an associated link when there is an attempt to access certain blocked sites or search for restricted content

Roles and Responsibilities

The **School Proprietor** has overall strategic responsibility for the filtering and monitoring of internet content and activity within the school and when using a school device. The Safeguarding Governer, the DSL and IT Manager are jointly responsible for ensuring that the expected standards for filtering and monitoring are met and evaluated regularly.

It is the responsibility of the **IT Manager**

- advise the Proprietor and the Senior Leadership Team on technical matters relating to filtering and monitoring, including hardware and software specifications and performance, relevant updates, new risks, etc.
- procure effective filtering and monitoring systems which sufficiently meet the school's needs and satisfies the expectations
- conduct the initial setup and ongoing maintenance of the filtering and monitoring systems
- manage system permissions agreed with Online Safety Team, including granting staff appropriate access within the monitoring software
- create and overseeing the filter 'white- and black-lists', to ensure the correct URLs are blocked, and access is given to those sites which have approval from SLT
- conduct monthly checks of filtering system, using a range of different devices
- contribute to the annual evaluation of the filtering and monitoring systems and procedures
- complete actions (e.g., amend filter and monitoring settings) following identified concerns, checks to the system or annual evaluation meetings

It is the responsibility of the **E-Safety Lead** to:

- Follows filtering and monitoring twice a day.
- Analyses NettSupport DNA twice a day. With daily analysis, it separates emergency situations and marks them in red, as well as follow-up situations, which it marks in yellow.
- If there is an emergency situation, it is immediately sent to the Safeguarding Team on two occasions during the day.
- Situations that need to be monitored are analysed at the end of each week (Friday) and then they can:
  - be removed from monitoring because they no longer cause concern
  - continue to follow up due to the frequency of repetition of the situation or the student
  - become urgent situations and turn red, when they are immediately delivered to the Safeguarding Team

- The weekly report must have several categories that the system recognizes and is analysed by the percentage of each category, the number of applications to the number of students and repetitions
- E-Safety Lead performs weekly filtering testing on randomly selected machines.

It is the responsibility of the **DSL and Safeguarding Team** to:

- regularly check the daily reports sent by the E-Safety Lead with the email name EMERGENCY E SAFETY (date and time) twice a day.
- regularly monitor weekly report sent by the E-Safety Lead in order to monitor any changes in situations that were only for monitoring.
- (with the Online Safety Team) review the effectiveness of the school's filtering and monitoring provision, as part of the Termly Safeguarding Review Meetings, and document any decisions made as a result.
- The Annual Safeguarding Review is conducted with the DSG, who will then relay any decisions or amendments to procedure to the Proprietor, if this has not been done already. It is important to note that further reviews of practice would be conducted at any time during the year if:
    - a safeguarding risk is identified
    - there is a significant change in working practice
    - new technology is introduced

- ensure that teaching staff:
    - are aware of the school's filtering and monitoring expectations
    - know how to report and record any filtering or monitoring concerns they may have observed or to which they may have been alerted
    - know how to request any amendments to the school filter's 'black- or white lists', wheren ecessary

It is the responsibility of the **teaching staff** to:

- monitor student online activity within their classroom
- ensure that the Behaviour policy or the *Safeguarding & Child Protection* policy procedures are followed, where relevant
    - email it_support@bis.edu.rs if the school's filter appears to be not working as expected on certain devices, accounts or locations.

Incidents

Any online safety incident involving a student is to be brought to the immediate attention of a member of the Safeguarding Team. They will then assist in taking the appropriate action to deal with the incident.

All incidents involving student online misbehaviour, failings to comply with the *Acceptable Use Policy* or safeguarding incidents, including cyber-bullying, must be reported. Online safety concerns where our existing systems fail to protect and fall short of expectations, e.g. viruses, spam and other breaches of security, must be reported immediately to the IT Technical Support it_support@bis.edu.rs.

Any concerns involving a member of staff's inappropriate use of technology should be reported to the relevant Head of School, in line with the school's Safeguarding & Child Protection Policy.

Record keeping

Records of online safety concerns where our existing systems fail to protect and fall short of expectations, e.g., viruses, spam and other breaches of security filters, as well as the resulting actions and outcomes, are logged in detail on the tickets that were sent to IT Technical Support email.

Training

It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, the BIS will hold an annual programme of training at the beginning of each new academic year, whereby they will be reminded of the *E-safety Safety Policy* and *Acceptable Use Policies.*
Any staff member joining the school part way through the academic year will be given individual induction training.

The Online Safety Team are responsible for giving recommendations for training and awareness raising for the school year to the Heads of Schools for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training, generally or in any particular area, this must be brought to the attention of the Heads of Schools for further CPD.

Curriculum

Online safety is taught specifically through the Computing and the PSHE curriculum, from EYFS to Year 11. Our online safety curriculum follows guidance from the DFE *'Teaching online safety in school'* publication. Furthermore, staff will ensure that the safe use of technology is encouraged and expected whenever ICT is used in the school, with risks highlighted and discussed when relevant. As well as scheduled online safety lessons, sessions will be planned and held in response to any current incident which may occur within a year group, e.g. cyberbullying. The school will also use assemblies to raise pupils' awareness of the dangers that can be encountered online and may invite speakers to talk to pupils about this.

In **EYFS,** we ensure our youngest leaners are respectful when using technology, as well as know what to do and who to talk to when they have a concern.

In **Key Stage 1**, pupils will be taught to:

- use technology safely and respectfully, keeping personal information private;
- identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage 2** will be taught to:

- use technology safely, respectfully and responsibly;
- recognise acceptable and unacceptable behaviour;
- identify a range of ways to report concerns about content and contact.

By the **end of Primary school**, pupils will know:

- that people sometimes behave differently online, including by pretending to be someone they are not;
- that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous;

- the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them;
- how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met;
- how information and data is shared and used online;
- how to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

In **Key Stage 3**, pupils will be taught to:

- understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy;
- recognise inappropriate content, contact and conduct, and know how to report concerns.

Pupils in **Key Stage 4** will be taught:

- to understand how changes in technology affect safety, including new ways to protect their online privacy and identity;
- how to report a range of concerns.

By the **end of Secondary school**, they will know:

- their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online;
- about online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online;
- not to provide material to others that they would not want shared further and not to share personal material which is sent to them;
- what to do and where to get support to report material or manage issues online;
- the impact of viewing harmful content;
- that specifically sexually explicit material (e.g., pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners;
- that sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail; how information and data is generated, collected, shared and used online;
- how to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.
- the positive use and dangers of AI

The safe use of social media and the internet will also be covered in other subjects where relevant.

The expectations listed above are in line with the *National Curriculum Computing Programmes of Study*;

The online safety curriculum will also be reviewed annually by the Online Safety Team and the Computing and PSHE teachers (Primary and Secondary), in order to ensure its content is relevant and up to date with current risks.

Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff will discuss cyber-bullying with their classes, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school *Behaviour Policy*. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

At present, Serbian schools **do not** have the same powers granted to UK schools with regards to being able to search for and, if necessary, delete inappropriate images or files on pupils' personal electronic devices (e.g., smartphones, tablets, laptops).

If the device is the student's personal device, staff can ask the student to show and/or delete the image or file in question if necessary. If the student is not compliant, the school will need to determine whether the child's parents and/or police should be contacted, depending on the severity of the concern. However, if the file is believed to be sexualised imagery of a minor, the image **must not** be viewed by any member of staff intentionally.

Youth-produced sexual imagery (sharing nudes and semi-nudes). For guidance relating to sharing nudes and semi- nudes, please refer to the *Safeguarding & Child Protection Policy*.

How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet and breaches the expectations identified in this policy, the relevant Acceptable Use Policies, we will follow the procedures set out in our Behaviour Policy, and disciplinary action may be taken. Any action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with our staff disciplinary procedures and Serbian Labour Law. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Remote learning

Due to the global pandemic (COVID19) our teachers, students and parents have been required to adopt remote learning techniques since March 2020. At BSB, our preferred and primary remote teaching and learning tools are those provided by Google for Education (e.g. Google Meet, Google Classroom, Google Drive, etc), although other premium online software is also used to complement the Google products.

As well as ensuring that we have the best possible online resources, we are committed to providing effective and safe practice for remote learning. See appendix 6 for our *Remote Learning Expectations*.