British School
of Bucharest

Online Safety Policy

Reviewed & Approved by	Senior Leadership Team
Last reviewed on	August 2019
Next review due by	August 2020

British School
of Bucharest

INTRODUCTION

At the British School of Bucharest, 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 'e-safety' incident, whichever is sooner.

This policy and the ***Staff Acceptable Use Policy*** is available for anybody to read on the British School of Bucharest website. These policies will also be made available with the Staff Handbook, and upon review all members of staff will sign to acknowledge that they have read and understood them. A copy of the ***Online Safety Policy*** and the ***Students' Acceptable Use Policy*** will be made available on the Parental Portal, along with the means to acknowledge agreement and permission. Upon receiving this acceptance of the terms and conditions, students will be permitted access to school technology including the internet.

For clarity, the ***Online 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.

AIMS

- To ensure that the requirement is met to empower the whole school community with the knowledge to stay safe and risk free.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

POLICY GOVERNANCE (ROLES & RESPONSIBILITIES)

HEADMASTER

A Reporting to the School Proprietor, the Headmaster has overall responsibility for online safety within our school in conjunction with the DSL. The day-to-day management of this will be delegated to the E-Safety Officers as indicated below.

The Headmaster will ensure that:

- online safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and parents;
- the designated E-Safety Officers have had appropriate CPD in order to undertake the day to day duties;
- all online safety incidents are dealt with promptly and appropriately.

E-SAFETY OFFICERS

The E-Safety Officers will

- keep up to date with the latest risks to children whilst using technology; familiarise him/herself with the latest research and available resources for school and home use;
- review this policy regularly and bring any matters to the attention of the Headmaster or a member of the Senior Leadership Team;
- advise the Headmaster and Senior Leadership Team on all e-safety matters;
- engage with parents and the wider school community on e-safety matters at school and/or at home;
- liaise with the IT Manager and other agencies as required;
- retain responsibility for reporting and recording e-safety incidents; ensure all parties know how and what to report and ensure

the appropriate audit trail;

- ensure any technical e-safety measures in school (e.g. internet filtering software and tools) are fit for purpose through liaison with IT Technical Support and other agencies;
- make themselves aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function and liaise with the Headmaster to decide on what reports may be appropriate for viewing.

IT TECHNICAL SUPPORT STAFF

The IT Manager 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 e-safety technical solutions, such as internet filtering, are operating correctly;
- 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 and should be alphanumeric;
- the deployment of a 2-step verification protocol for all staff Microsoft accounts;
- the IT System Administrator password is to be changed on a four-monthly basis, or earlier if the password's security is suspected of being compromised in any way.

ALL STAFF

Staff are to ensure that:

- all details within this policy are understood. If anything is not understood it should be brought to the attention of an E-Safety Officer or a member of the Senior Leadership Team;
- any e-safety incident is reported to an E-Safety Officer, or in their absence to a member of the Senior Leadership Team, and an e-safety incident report is made (on iSAMS under 'Cause for Concern'). If you are unsure, the matter is to be raised with an E-Safety Officer or a member of the Senior Leadership Team to make a decision;
- the reporting flowcharts contained within this Online Safety Policy are fully understood (see appendix).

ALL STUDENTS

The boundaries of use of ICT equipment and services in this school are given in the ***Students' Acceptable Use Policy*** (each age-related version); 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.

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, 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. The school will also provide clear guidance as to how they can seek further online safety advice or report an online safety concern or incident. Parents should also understand that the school needs to have rules in place to ensure that their child can be properly safeguarded. As such, parents will be required to sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

British School
of Bucharest

E-SAFETY COMMITTEE

Chaired by the Headmaster, the E-Safety Committee is responsible:

- to advise on changes to the Online Safety Policy;
- to establish the effectiveness of online safety training and awareness in the school;
- to recommend further initiatives for online safety training and awareness at the school.

Established from E-Safety Officers, IT Manager, selected members of Student Voice, volunteer parent(s) if possible and others as required, the E-Safety Committee will meet on a bi-annual basis.

TECHNOLOGY

The British School of Bucharest uses a range of devices including PC's, laptops, Apple Macs, Chromebooks and iPads. There is also a ***Bring Your Own Device scheme*** in operation across Years 12 and 13. In order to safeguard students and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use Squid Guard software that prevents unauthorized access to illegal and inappropriate websites, identified through http://www.shallalist.de. The IT Manager and the E-Safety Officers are responsible for ensuring that filtering is appropriate and that any issues are brought to the attention of the Headmaster or a member of the Senior Leadership Team. BSB also uses Securly as a filtering and monitoring tool for all student activity whilst they are logged into their BSB Online accounts. Any flagged activity will be immediately reported via automated email to designated Senior Leaders and E-Safety Officers.

Email Filtering – we use Office365 in the Cloud that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email, such as a phishing message.

School Sensitive Information – If staff have established access to school accounts via their personal devices, e.g. email and cloud accounts, the school reserves the right to delete all information within these accounts in the case of an emergency, whereby sensitive data is no longer secure. This may include the staff member's personal data and content, if this has been stored within the school account. With all data, BSB complies with GDPR expectations.

Passwords – all staff and students will be unable to access their personal school account without a unique username and password. Staff and student passwords will change on a four monthly basis 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 the iPads. Nevertheless, all staff and students are required to log in to their school server account or BSB Online account in order to store their work. All staff and students must also ensure that they log out of their accounts when finished.

Two-Step Verification – The management of individual passwords is also protected securely using a two-step verification system, either via text message to a designated phone number provided by each user or via email using an alternative email address. Two-step verification will be required when logging into each Microsoft web-based app (Outlook, OneDrive, SharePoint, etc) on a new device or browser.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. The IT Manager will be responsible for ensuring this task is carried out and will report to the Headmaster if there are any concerns. All USB peripherals such as key-drives are to be scanned for viruses before use.

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 (AUP). This will be done by signing the Staff Handbook, which contains the Staff AUP. Internet use will be granted to students once their parents have agreed to the terms of the relevant* Student Acceptable Use Policy, via the Parental Portal, and the students themselves have signed** the Class/Form Acceptable Use Policy poster, which will be displayed in the classroom throughout the year.

British School
of Bucharest

*There are two age appropriate Student AUPs: EYFS & KS1; KS2 and Secondary.

**EYFS students are not required to sign.

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 BSB Online account and as such will be given their own email address. The email address can be activated if required and will be their first name, followed by a dot, followed by their surname, followed by @bsbonline.net, e.g. jack.smith@bsbonline.net.

PHOTOS AND VIDEOS – Digital media such as photos and videos are covered in the schools' Parent Handbook, and is reiterated here for clarity:

Photographs/Fotografii

Occasionally photographs of the students are used on the website or in BSB publication materials (e.g. BSB Newsblast). To protect our students, we do not publish their full name and photograph together, we ensure children are appropriately clothed for photographs and we do not allow commercial or media photographers to have unsupervised access to pupils.

By signing the Registration File, parents/guardians give consent for the school or someone commissioned by the school to take and use photographs and video recordings for educational purposes, to record events and to publicise the work of the school on our website, social media channels, in the school or through a prospectus, or local, national or international media. If you do not wish your child's photographs to be used for such purposes, you will need to indicate this in the registration documents.

Students are not permitted to use a portrait photograph of themselves as their 'login image' for internet accounts, such as BSB Online, as their email address will contain their name.

Social Networking – there are many social networking services available; the British School of Bucharest 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. The following social media services are permitted for use within the British School of Bucharest and have been appropriately risk assessed: EduBlogs/Wordpress, Twitter and Facebook.

Should staff wish to use other social media, permission must first be sought via an E-Safety Officer who will advise the Headmaster for a decision to be made. Any new service will be risk assessed before use is permitted. All three social media services that the British School of Bucharest use are employed as a broadcasting service. A broadcast service is generally used as a one-way communication method in order to share school information with the wider school community. The Friends of BSB Classlist App does allow for two-way communication, however, access and all comments are moderated.

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;
- where services are 'comment enabled', comments are to be set to 'moderated';
- all posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and takedown policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

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
- Edmodo
- Showbie
- ShowMyHomework
- Padlet

It is a privilege for students to use these online school services and tools and all posts and uploads to them are monitored. Any deviation or misuse of these services or tools will be dealt with in accordance with the Behaviour Policy.

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. Consequently, moderated age-appropriate search engines are used where possible. 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.

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 BSB Online accounts, student activity can be monitored using the web tool Securly.

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 Student AUP to inform parents, openly inviting any questions regarding the matter.

Incidents – Any online safety incident involving a student is to be brought to the immediate attention of an E-Safety Officer, or in their absence, a member of the Senior Leadership Team. They will then assist in taking the appropriate action to deal with the incident and the incident log will be filled in.

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 British School of Bucharest will hold an annual programme of training at the beginning of each new academic year, whereby they will be reminded of the Online Safety Policy, the Acceptable Use Policies and the ***Online Safety Reporting Procedures***. Any staff member joining the school part way through the academic year will be given individual training.

Parent workshops (age appropriate) will be held during the Autumn term, as early as possible, offering advice and support, as well as outlining the school's expectations.

As well as the programme of training, we may establish further training or lessons as necessary in response to any incidents.

The E-Safety Officers are responsible for recommending a programme of training and awareness for the school year to the Headmaster and Heads of Primary and Secondary 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 Headmaster or Heads of Primary and Secondary for further CPD.

Curriculum – Online safety is taught specifically through the Computing and the PSHCE curricula, from EYFS to 6th Form. Our online safety curriculum follows guidance from the DFE 'Teaching online safety in school' publication, as well as the UKCCIS 'Education for a Connected World' document. 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. Particular emphasis is also given to online safety awareness on 'Safer Internet Day' each February. The online safety curriculum will also be reviewed annually by the E-Safety Officers and the Computing and PSHCE Subject Leaders (Primary and Secondary), in order to ensure its content is relevant and up to date with current risks.

British School
of Bucharest

GUIDANCE ON OTHER RELATED ONLINE SAFETY MATTERS

For specific online safety issues, such as sexting and online radicalisation please refer to the school's Safeguarding and Child Protection Policy, the school's Prevent Duty Policy, as well as the government non-statutory guidance on these matters.

Related Policies & Documents

- Acceptable Use Policies
- Online Safety Incident Reporting Procedures
- Online Safety Risk Assessment
- Online Safety Incident Log (on iSAMS)
- Safeguarding and Child Protection Policy & Whistleblowing Policy
- PSHCE Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Handbook
- Parent Handbook

This policy has also been translated into Romanian.

British School
of Bucharest

ACCEPTABLE USE POLICY – STAFF

Note: All internet and email activity is subject to monitoring.

You must read this policy in conjunction with the Online Safety Policy and the school's Social Media Guidance. Signing the Staff Handbook acknowledges that you have read and understood these documents and the expectations outlined within them.

Internet access – You should not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an online safety incident, reported to an E-Safety Officer and an incident sheet should be completed.

Social networking – is allowed in school in accordance with the online safety and social media policies only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become 'friends' with or 'follow' pupils on personal social networks. If staff 'friend/follow' any parents over social media, all communication must remain professional and should not relate to any school matters.

Use of 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.

Passwords – All devices, personal or otherwise, that contain or can access school information, require a password, pin or other form of security in order to prevent illegal access, in case of theft or loss. Furthermore, staff should keep passwords private. There is no occasion when a password needs to be shared.

Data Protection – On no occasion should data concerning sensitive personal information be taken off-site on an unprotected device (USB Drive, etc). All sensitive personal information should remain on one of the secure school systems with the appropriate user access permissions.

Personal Use of School ICT – You are not permitted to use school ICT for personal use unless specific permission has been given from a member of the Senior Leadership Team, who will set the boundaries of personal use.

Images and Videos – You should not upload onto any public internet site or service images or videos of other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal ICT – Using personal ICT is at the discretion of the Senior Leadership Team. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by an E-Safety Officer.

Viruses and other malware – any virus outbreaks are to be reported to Helpdesk as soon as it is practical to do so. Helpdesk will then contact any suitable external agencies, if necessary.

Online Safety – online safety, or e-safety, is the responsibility of everyone to everyone. As such you will promote positive online safety messages in all use of ICT, whether you are with other members of staff or with students.

British School
of Bucharest

ACCEPTABLE USE POLICY – KS2 & SECONDARY STUDENTS
OUR AGREEMENT OF GOOD ONLINE BEHAVIOUR

Note: All internet and email activity is subject to monitoring.

I Promise – to only use the school ICT for schoolwork that a teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting or unsafe.

I Promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.

I will not – damage school ICT purposely. If I accidentally damage something I will tell my teacher or TA.

I will not – share my password with anybody. If I forget my password, I will let my teacher or TA know.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – capture and/or share images or video of others without their permission.

I will not – download anything from the internet unless my teacher has asked me to.

I will – let my teacher or TA know if anybody asks me for personal information.

I will – let my teacher or TA know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online; I will treat everybody the way that I want to be treated.

I understand – that some people on the internet are not who they say they are, and some people can be unkind. I will tell my teacher or TA if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this agreement there will likely be consequences for my actions and my parents will be told.

British School
of Bucharest

ACCEPTABLE USE POLICY – EYFS & KS1 STUDENTS
OUR AGREEMENT OF GOOD ONLINE BEHAVIOUR

Note: All internet and email activity may be monitored.

I promise - to always be very careful when using school ICT and to tell my teacher or TA if I damage anything accidentally.
I promise - that I will only do the activity the teacher has asked me to do when using school ICT.
I promise - not to look for or show other people things that may upset them.
I promise - that I will tell the Teacher or TA straight away if I ever see anything upsetting on school ICT.
I promise - to be kind when using school ICT.

School ICT - the computers, iPads, Chromebooks and other technology in school.

British School
of Bucharest

APPENDIX: ONLINE SAFETY INCIDENT REPORTING PROCEDURES