BRITISH INTERNATIONAL SCHOOL

E-Safety Policy

Development / Monitoring / Review of this Policy

This E-Safety policy has been developed by a working group made up of:

- Directors
- Senior Management
- Staff – including Teachers, Support Staff, Technical staff
- E-Safety Officer

The implementation of this E-Safety policy will be monitored by the Senior Management Team. Monitoring will take place at regular intervals: at the start of each academic year.

The E-Safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity

Scope of the Policy

This policy applies to all members of the school (including staff, students, volunteers, parents / carers, visitors) who have access to and are users of the school's ICT systems, both in and out of the school.

The Head of School will also regulate the behaviour of students when they are out of school and empower members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school.

Directors

Directors and the Governing body are responsible for the approval of the E-Safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Directors receiving regular information about e-safety incidents and monitoring reports.

E-Safety Officer

E-Safety Officer's responsibilities will include:

- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Directors / Board
- taking day to day responsibility for e-safety issues and having a leading role in establishing and reviewing the school e-safety policies / documents
- ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- providing training and advice for staff
- liaising with the relevant body
- liaising with school technical staff
- receiving reports of e-safety incidents and creating a log of incidents to inform future e-safety developments
- managing implementation of software required to ensure the provision of E-Safety in the school

Head of School and Senior Leaders

The Head of School has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Officer (Mr. Certic).

The Senior Management Team is responsible for ensuring that any relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

Technical staff

The IT Manager / Technical Staff is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- high quality web-filtering is applied and updated on a regular basis and that its implementation is sole responsibility of the E-Safety officer
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / any virtual learning environments / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal for investigation
- that monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they report any suspected misuse or problem to the E-Safety Officer for investigation

- all digital communications with students / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the e-safety and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead (DSL)

Best practise indicates that DSL should be trained in e-safety issues and be aware of the potential for serious student protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

They should also have a reasonable awareness of the most popular platforms used by students and how these may be implicated in the above issues.

Students

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital capture devices. They should also know and understand policies on the taking / use of images and on cyber-bullying
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety policy covers their actions out of school, if related to their membership of the school.

Parents / carers

Parents / Carers play a crucial role in ensuring that their child understands the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, blogs and other relevant information. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / blogs and on-line student pictures
- their child's personal devices in the school (where this is allowed)

They should also have a reasonable awareness of the most common platforms used by their children and how these may be implicated in the above issues.

Students' Education

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Students and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing/ ICT/ Computer Science / PSHE / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable (made in writing by email), with clear reasons for the need.

Technical Equipment Filtering and Monitoring

- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must as safe as possible
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by Mr A Certic who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Head of School
- Aca Certic (IT Manager and E-Safety officer) is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could

cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)

- Internet access is filtered for all users. Illegal content (child/ animal sexual abuse images) is filtered by the broadband or filtering.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Where staff or students use non-school internet services (e.g. mobile phone 4G signal) the school cannot control for content or effect filtering.

Bringing Your Own Device

- The school has a set of clear expectations and responsibilities for all users
- All users are provided with and accept the Acceptable Use Agreement
- All internal network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school’s normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Best practise indicates that training be undertaken for all staff
- Students receive training and guidance on the use of personal devices
- Any device loss, theft, change of ownership of the device will be reported
- All devices are brought to the premises at the owners own risk
- Misuse of devices may result in these being temporarily confiscated

Use of Digital Images and Video

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Parents / carers are welcome to take videos and digital images of their students at school events for their own personal use. To respect everyone’s privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used without express permission of senior leaders (written/ email)
- Video images captured during remote teaching and learning will be used for safeguarding purposes only - see BIS Policy for recording video conference lessons.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission (in accordance with Serbian data protection law)

- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers should be obtained before photographs of students are published on the school website (see Appendix 1)
- Student’s work can only be published with the permission of the student and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the UK Data Protection Act 1998 and in line with pertinent Serbian law (where Serbian law differs from UK guidance, Serbian law will always take precedence), which states that personal data will be:

- Fairly processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject’s rights
- Secure
- Only transferred to others with adequate protection

The school will ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing” (Serbian data protection law)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties

Staff must ensure that they:

- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (once it has been transferred or its use is complete

The school also complies with Serbian data protection law (2019) in cases where it is more stringent than or supersedes the above data protection information from the UK. This particularly applies to the storage and dissemination of data and other information held by the school.

Policy Review

This policy is reviewed annually.
Reviewed July 2021

Appendix 1

Permission to Use Student's Photographs

Dear Parents/Guardians,

Students at the British International School will be involved in school activities where they may be photographed. Photographs of students may be used in a variety of media to celebrate a student's success in a particular area, for educational purposes or to promote activities at the school. Photographs of children are also used in newspapers, school brochures, school website, school DVD, special displays and other promotional material.

The majority of parents are happy for their child's photograph to be used and their children enjoy seeing their photographs in the newspapers and on school publications.

We need parental permission to publish children's photographs. No child's photograph will knowingly be published without parental permission. Accordingly, I ask that you complete the form below and return it to the school as soon as possible.

Please note this permission form is valid for the duration of your child's schooling at the British International School; however permission may be withdrawn at any time upon written notification.

Thank you

Aleksandra Keserovic
Director of Education

PERMISSION TO USE STUDENT'S PHOTOGRAPHS

Student's Name: ____

Year: _______________

1. Permission for photographs of my child to be published in local media, used in advertising materials or special displays, and I am aware that this may be accompanied by my child's first name.

INDIVIDUAL	GROUP	WIDE VIEW
Y / N	Y / N	Y / N
Y / N	Y / N	Y / N
Y / N	Y / N	Y / N

*Individual: photograph showing your child's face as the main face or one of the main faces.

* Group: showing your child's face as a part of a group.

*Wide view: showing your child in a larger group setting. This may not show your child's face but they still may be identifiable.

2. Permission for my child's photograph to be used in the British International School newsletter, DVD and school website.

INDIVIDUAL	GROUP	WIDE VIEW
Y / N	Y / N	Y / N
Y / N	Y / N	Y / N
Y / N	Y / N	Y / N

3. Permission for my child to appear in school marked activities with their face blurred or not identifiable.

INDIVIDUAL	GROUP	WIDE VIEW
Y / N	Y / N	Y / N
Y / N	Y / N	Y / N
Y / N	Y / N	Y / N

I acknowledge that ownership of such material is retained by the school.

Parent/Guardian Name:____

Signature: _________________________________ Date:_______________________

Appendix 2

Contacts for local legislation on E-Safety and Safeguarding:

Contact names	
Designated Safeguarding Lead (DSL)	Jelena Milicevic
Assistant Designated Safeguarding Lead (ADSL)	Ljubica Stankovic

Third Party contacts	
Local authority social services contact page	http://gcsrbg.org/contact-us/
[Local Authority] Designated Officer for child protection	Sadija Gicic and Snezana Stojanovic
Local authority's out of hours contact numbers (Social services call centre)	011/2650 542
Where there is a risk of immediate serious harm to a child a referral should be made to children's social care immediately by the DSL. If a child is in immediate danger, ring 192.	
Local Police Emergency	192
Local Police non-emergency	011/361 8744

See Safeguarding Policy for further sources of support and advice.