AZERBAIJAN BRITISH COLLEGE
EXPLORE TO ACHIEVE

# E-Safety Policy

Revised June 2022

E-safety or internet safety is the concept of protecting our community as they navigate the internet, especially those most vulnerable. It tries to protect users from potentially harmful content that can be found on apps or websites, or the effects of such content, such as grooming, pornography, or cyber bullying. In practice, e-safety is as much about behaviour as it is electronic security. E-safety in this context is classified into three areas of risk:

- **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.

At the ABC our aims are to:

- to protect and educate pupils and staff in their use of technology
- to have the appropriate mechanisms to intervene and support any incident where appropriate.

## Development / Monitoring / Review of this Policy

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

- The Board of Directors
- Senior Leadership
- Staff – including Teachers, Support Staff, Technical staff

The implementation of this E-Safety policy will be monitored by the respective Heads of School. 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 Azerbaijan British College (ABC), including staff, students, volunteers, parents and visitors, who have access to school's ICT systems, both in and out of the school.

The Heads of Schools (HoS) 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 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.

## Board of Directors

The Board members 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.

## Heads of School and Heads of Key Stages

The Heads of Schools (HoS) have 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 and Heads of Key Stages (HoKS).

The HoKS as leads for e-safety are responsible for ensuring:

- 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 eventof 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 futuree-safety developments
- managing implementation of software required to ensure the provision of E-Safety inthe school

## Technical staff

The IT Manager / Technical Staff are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- to monitor internet regularly and make sure that there are no 'fake' ABC related pages or pages that compromise the e-safety of our students
- 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 itsimplementation 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 bereported to the Principal for investigation
- that monitoring software / systems are implemented and updated

## 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-safetypolicy and practices
- they report any suspected misuse or problem to the HoKS for investigation

- all digital communications with students / parents 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) and Deputy Designated Safeguarding Leads (DDSL)

Best practise indicates that DSL/DDSL should be trained in e-safety issues and be aware of the potential forserious 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

Parents 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 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/phones

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 ICT/ PSHCE lssons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies andtutorial / 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 mobiledevices
- 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 monitoringthe content of the websites the young people visit.

## 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 IT support services 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 IT Manager is responsible for ensuring that software license logs are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations
- Internet access is filtered for all users. Illegal content 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 e.g. on social networking sites.
- 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)
- 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
- 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 should be obtained before photographs of students are published on the school website (see Appendix 1).

# Appendix 1

## *Permission to Use Student's Photographs*

Dear Parents/Guardians,

Students at Azerbaijan British College will be involved in school activities where they may be photographed. Photographs of students may be used in a variety of media for educational purposes, to celebrate success or to promote activities at the school. Photographs of children are also used in newspapers, school brochures, school website, 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 media 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 theform 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 Azerbaijan British College; however permission may be withdrawn at any time upon written notification.

Thank you

Carl P Lander
Principal

**PERMISSION TO USE STUDENT'S PHOTOGRAPHS**

Student's Name: _____ Year & Class: _____

Please tick ONE box.

I hereby give permission for the image of my child to used by the school ☐

I do not give permission for my child's image to be used by the school ☐

.

Parent Name:_____

Signature:_____Date:_____

## Appendix 2

*Contacts for local legislation on E-Safety and Safeguarding:*

| **Contact names** | Preschool | Primary School | Secondary School |
|---|---|---|---|
| Designated Safeguarding Lead (DSL) | Ms Nilufer Hasanli | Mr William Glover | Mr Nicholas Taylor |
| Deputy Designated Safeguarding Lead (DDSL) | Ms Nurlana Guliyeva | Ms Gunay Huseynli | Ms Hijrana Aliyeva |

See Safeguarding Policy for further sources of support and advice.