BRIGHTON COLLEGE
DUBAI

# E-Safety Policy

Please see Brighton College Dubai Policies and Guidelines

## 1. Introduction

Brighton College Dubai is committed to doing all it can to keep pupils safe, including whenever they are online. The College is committed to making a full and innovative use of the internet and other forms of electronic communication and technological developments. The College acknowledges that alongside the wonderful educational benefits and advantages, there is also the potential for misuse and harm. The College accepts the challenge of educating the College community to be wise and considerate users of technology, as well as emphasising that the internet should not be used inappropriately or illegally.

The policy provides an overview of how the school seeks to address E-Safety.

The other relevant policies, to be considered alongside this policy, are:

- Pupil BYOD, iPad and Technology Acceptable Use policy
- Bloom Education Information Security Handbook
- Safeguarding and Child Protection policy
- Positive Behaviour policy
- Anti-bullying policy

## 2. Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, parents, visitors) who have access to and are user of the College's technology systems, both in and out of the College. The College will deal with E-Safety incidents in accordance with the procedures outlined in both this policy and in associated College policies, such as the safeguarding and child protection, positive behaviour and anti-bullying policies. It will, where known and appropriate, inform parents of incidents of inappropriate E-Safety behaviour that take place out of the College.

## 3. E-Safety: The College's Role

Brighton College Dubai take issues related to E-Safety extremely seriously and takes the following steps to help educate, inform and assist pupils in the area:

## 3.1 Education – a focus on wisdom

Encouraging and enabling pupils to make wise choices for themselves when on-line, even when no one is looking, underpins our approach to e-safety education in the College. With the relatively recent development in 4G and 5G technologies, this has become an even more vital approach to E-safety, educating pupils to take responsibility for making their own choices and even more so when pupils are bringing their own devices into the College and connecting to the network.

All staff work closely together to ensure that:

- The College reinforces internet safety messages to pupils at regular intervals and at an age-appropriate level through computing lessons, Moral Education, PSHE lessons, tutor time and assemblies. Issues covered include topics of the following nature: safe and appropriate use of social networking sites; the issues surrounding excessive use of games consoles, internet gaming sites; mobile phones and social networking or messaging facilities; the sending of inappropriate photos via mobile phone or the Internet; the effect on pupils' wellbeing and self-image of social media and other messages that they may get from online activity; the effect of inappropriate content of pupils' self-image and their relationships with others.

All members of the College community are informed of the College's Acceptable Use Policy, which explains their responsibility for safe and appropriate use of the College's computer systems and their own devices. All staff and pupils have to sign the relevant Acceptable Use policy on entry of the college.-Parents are made aware of the BYOD and iPAD Acceptable Use Policy as part of the admissions process. This is a key document that needs to be signed and submitted prior to pupils joining the College.

### 3.1.1 Education and Pupils

E-Safety should be a focus in all areas of the computing curriculum and staff should reinforce E-Safety messages across various curriculum topics. E-Safety is a broad topic area and will be covered in the following ways:

- Through key PSHE themes such as Digital Literacy, Transition and Safety, Exploring Influence. These topic lists are reviewed annually
- Key E-Safety messages are reinforced as part of a planned programme of assemblies
- Pupils are taught to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information in computing lessons and cross curricular
- Pupils are helped to understand the need for the pupil Acceptable Use Policy agreement and encouraged to adopt safe and responsible use both within and outside school

- Pupils are helped to understand the benefits and risks associated with social media, online posting and message
- Pupils are informed how they can report an issue on-line, both externally and within school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics that would normally result in internet searches being blocked. In such a situation, staff can request IT Support to remove those sites from the filtered list for those pupils.

### 3.2.1 Education and Parents

Parents play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours, and the College seeks to build an effective partnership with parents. As part of the KHDA Parent Contract with Brighton College Dubai, parents agree to follow and comply with all College policies and protocols, including the E-Safety Policy.

The College provides information and awareness to parents through the College Newsletters, workshops and other communication as appropriate. As part of the workshop series for parents, there is an annual Online Parent Safety Workshop delivered by the Head of Computing and College Counsellor, to which all parents are invited. The notes from the session are made available to parents.

The following advice for parents is drawn from recommendations made by the Child Exploration and Online Protection Centre (CEOP):

- Make yourself aware of the amount of time your child is using the Internet, chat facilities, games consoles and their mobile phones and whether this is excessive.
- Consider carefully the location of the computer or laptop and whether your child would be better using it in a family area of the home
- Consider whether it is wise for them to have their phone or device with them when they go to bed
- Search on Google and other search engines for your child's name and any online usernames they use. This is a valuable exercise for you and them to see exactly how much other people can see about them with very little difficulty
- Consider installing Internet monitoring software on your home computer(s) and devices
- Talk to your child; both about the dangers or the Internet, but also about their general usage – be interested in what they are doing and keep a dialogue open to they feel able to talk to you in they do experience problems
- Make sure they know how to report a problem or an inappropriate image/comment

- Ask your child to (or help them) set up appropriate privacy settings on social networking sites (please contact the College if you need help or advice in this area)

## 3.2 Staff Responsibilities

The Subject leader of Computing works very closely with staff to ensure that there is suitable and effective provision for staff and pupils relating to E-Safety.

All staff are required to complete Staying Safe Online for International Schools training through EduCare. The Designated Safeguarding Lead (DSL) is trained, along with the Deputy DSLs, in E-Safety issues and made aware of the potential for serious child protection and safeguarding issues.

## 3.3 Filtering and Monitoring

- The College technician ensures that the network uses filtering software, which amongst other things restricts access to social networking and gaming sites, as well as key words and inappropriate images or videos. Access to sites such as YouTube is also limited, and the material available through such sites restricted.
- Pupils and staff are encouraged to share any sites that need to be filtered or that have not
- Pupils are not allowed to use the guest connection and have their own accounts which is monitored by ICT Support
- The College use Fortinet as our firewall filtering and monitoring provider.
- We actively try not to 'over-block' internet access on the College system

## 3.4 Networking and Infrastructure

- Significant investments have been made by the College to ensure that the school's network is fast, secure and reliable.

## 3.5 Discipline/Sanctions

- We follow the appropriate College disciplinary procedures in relation to any incident of misuse of technology equipment or websites or of cyber bullying and other inappropriate behaviour on-line. The College reserves the right to take action – even when the offence is committed outside of College – if it harms members of our community or brings the College into disrepute.

## 4. Expectations on Pupils

### 4.1 Pupil BYOD, iPad and Technology Acceptance Use Policy

Pupils are responsible for using the College digital technology systems in accordance with the Pupil AUP Agreement. They:

- 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 cameras. They should also know and understand policies on the taking and use of images and on cyber-bullying.
- the college has a zero-visibility approach on mobile phones throughout the school day. We acknowledge that pupils will have mobiles phones in their possession for contacting parents at the end of the school day, however they must be visible or used throughout the school day.
- should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the College's E-Safety Policy covers their actions out of school, if related to their membership of the school.

These are set out in the Pupils' Acceptable Use Policy, and every pupil or parent has to sign this during the admissions stage.

### 4.2 College computers and College network

The computer suite should only be used when there is a member of staff present and the rules posted in each room must be observed. Any attempt to abuse or interfere with the network or any College computer equipment will be regarded as an extremely serious offence and may result in a pupil losing their place at Brighton College Dubai. All computer activity in the College is monitored. Pupils did not have access to USBs and this is disabled for pupils

### 4.3 Pupil use of the internet, e-mail and other digital technology

The school views very seriously any use of the Internet, e-mail and any other digital media or technology to bring the College name into disrepute, to cause hurt or distress to others, or to have a negative impact on the College community in any way. Any pupil found to have misused technology in such a manner faces losing their place at Brighton College Dubai. The College's view applies whether or not a pupil is on the College premises, in the care of the College, wearing College uniform, on a College activity, and whether it is during or outside the College.

### 4.4 Social media and networking sites

The College does not discourage pupils' use of social networking sites, providing this is done safely and with due consideration for others, themselves and the College. Advice is given to pupils on this subject via PHSE lessons, assemblies and outside speakers. Clear guidance on setting and how to stay safe on social media sites can be accessed through the E-Safety page on the school intranet, which is updated regularly and highlighted to pupils by tutors. No pupil should post photos, video clips or comments that could in any way be considered as harassment or an invasion of privacy, or which are embarrassing and hurtful. In general, pupils should always ensure that they have secured the permission of anyone about whom they intend to posit material. Equally, they should not post anything that could in any way conflict with the ethos and aims of the school or that brings the school into disrepute.

## 4.5 Specific Issues

### 4.5.1 Cyber-bullying

Cyber bullying is an aggressive, intentional act carried out over a period of time, by a group or individual using electronic forms of contact, against a victim who cannot easily defend him/herself. Mobile, Internet and wireless technologies have increased the pace of communications and brought benefits to users worldwide. Unfortunately, however, their popularity provides the opportunity for misuse through cyber bullying. This might include:

Text message bullying
Picture/video bullying via mobile phone cameras
Phone call bullying via mobile phone
Email bullying
Chat room or social network bullying
Bullying through instant messaging
Bullying via websites
The withholding of approval (e.g., not liking an image/post)

Cyber bullying is explicitly referred to in Brighton College's Anti-bullying Policy. The College's expectations of pupils are clearly communicated to them in the Pupil Code of Conduct, College assemblies and PSHE lessons are also used to update pupils on relevant cyber issues and how to find help or support. Pupils are given clear instruction and guidance about the nature of 'banter' and the need to consider the consequences of words spoken, jokes made and in particular, the dynamic of who and how many others are making 'jokes' at someone else's expense.

The Positive Behaviour policy makes it clear that bullying behaviour will usually lead to a pupil's place at school being removed.

Sexting

Whilst professionals refer to the issue as 'sexting' there is no clear definition of 'sexting'. Many professionals consider sexting to be 'sending or posting sexually suggestive images, including nude or semi-nude photographs, via mobiles or over the Internet. Yet, when young people are asked 'What does sexting mean to you?' they are more likely to interpret sexting as 'writing and sharing explicit message with people they know'. Similarly, many parents think of sexting as flirty or sexual text message rather than images.

The school makes it clear that forms of sexting may constitute making, strong or sending of child pornography. The Head Master also specifies that sexual activity on the school grounds, including sexting, may result in a pupil being asked to leave the school.

The Designated Safeguarding and Deputy Leads will liaise closely with the relevant Head of Section regarding appropriate pastoral and disciplinary responses to incidents of sexting.

Radicalisation

Protecting children from the risk of radicalisation is seen as part of the school's wider safeguarding duties and is similar in nature to protecting children from other forms of harm and abuse. During the process of radicalization, it is possible to intervene to prevent vulnerable people being radicalised. There is no single way of identifying an individual who is likely to be susceptible to an extremist ideology. It can happen in many different ways. Specific background factors may contribute to vulnerability which are often combined with specific influences such as family, friends or online. The internet and the use of social media in particular has become a major factor in the radicalization of young people. The College reinforces radicalisation messages to pupils at regular intervals and at an age-appropriate level through computer science lessons, Moral Education, PSHE lessons and assemblies.

## 5. Expectation on Staff

### 5.1 Staff understanding of expectations on pupils

It is vital that staff understand the College's expectations of pupils in relation to E-Safety issues, and these are made clear to staff in the following ways:

- Through guidance on the College policy in the area in the Staff Handbook
- Through the annual safeguarding training for all staff
- Through updates on cyber issues during in-service training (INSET) days and staff meetings

- Through the induction programme for new members of the teaching staff
- Through announcements at weekly staff briefings, via whole School e-mails, and through information passed on to form tutors
- Through pastoral meetings held regularly

## 5.2 Staff Conduct and Acceptable Use

Staff behaviour and conducts on-line, both in school and in their own time, should comply with the Bloom Education information Security Handbook policy and the staff code of conduct in the Staff Handbook.

As with all behaviour towards pupils, all staff must ensure any electronic communication they have with pupils is appropriate and should use common sense in judging how to approach a given situation. Staff should be aware of the expectations within the Staff Handbook. Some of these which are written below:

- Do not give your personal contact details, including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with a member of CLT and the pupil's parents.
- Do not share or store personal mobile numbers of pupils on personal mobile phones. If you must make phone contact with a pupil (e.g., on a school trip), it is a good idea to use a school mobile to do so. If this impossible, then any pupil's contact details should be deleted from the personal mobile phone as soon as the trip is over.
- Use iSAMS to send emails and school equipment, where possible, for taking photographs.
- Delete any pupil data you have temporarily stored on your personal phone (e.g., a photo for the Newsletter) as soon as it is no longer needed.
- Be prepared to demonstrate that any pupil data captured on your personal equipment has only ever been used for professional, school-based purposes.
- It is important to keep phone contact and e-communication formal and professional at all times
- School e-mail addresses should always be used
- Do not use internet or web-based communication channels to send personal messages to pupils and ensure that, if a social networking site is used, details are not shared with children and young people and that privacy settings are set at a maximum. Do not, for example, befriend pupils on Facebook or similar social media forums. Think carefully before "friending" former pupils, especially those with friends who are current pupils, or siblings of current pupils – we strongly recommend at least a two-year gap before even considering 'friending' former pupils
- Do not view photographs or videos on an electronic device that you have confiscated from a pupil. If you must confiscate a device, hand it to the Deputy Head, having asked the child to switch it off. (CLT may search a pupil\s electronic device in certain situations). If there is a suggestion that the material may be related to a child protection matter, the device should be handed immediately to the DSL.

Staff should not communicate with pupils outside the hours of 7:00am to 6:00pm, unless required within the context of a college residential trip.

## 6. Training of Staff

Staff will receive guidance and training relating to E-Safety on a regular basis, both through formal INSET meetings, and through e-mail or briefing updates circulated.

## 7. Monitoring and Review

This policy is monitored on a termly basis by the Head Master and is reviewed annually by the Board of Governors.

## 8. Approved by

Head Master on behalf of the College:

Simon Crane, Head Master

On behalf of the Governors:

Mrs Nilay Ozral, Board Member

## Change History Record

| Version No. | Description of Change | Owner | Date of Issue |
|---|---|---|---|
| 1.0 | Policy edited and updated | **Joe Donaghey** | **May 2022** |
| | | | |

## Brighton College Dubai Policies and Guidelines

**Policy Statement**
Brighton College Dubai policies have been developed by the College Leadership Team (CLT) with input and guidance from the Brighton College network, including Brighton College UK.

Policies reflect current best practice.

At the time of writing, policies aligned with the following:

- KHDA Guidance and Guidelines for Private Schools
- MOE United Arab Emirates School Inspection Framework
- DSIB School Inspection Supplement
- The College's Academic Plan written for KHDA approval
- Standards for British Schools Overseas (DfE)
- COBIS Accreditation and Compliance
- Bloom Education and Bloom Holding policies where applicable

Should any regulations change or develop further, the policies will be reviewed to ensure continued alignment.

**Policy Structure**
Policies will show the date of writing and reviews on them. Version control will also be in place. Should there be an error or inaccurate fact in any policy, a CLT member should be notified.

**Policy Development**
Policies will continue to be developed as strategic priorities are set.