The British School of Bahrain
Blended Learning Environment during COVID-19

E-Safety Policy

Policy Reference: COVID – E Safety Policy
Distribution: Whole School
Author: Executive Headmaster
Approved by: Board of Trustees
Date adopted: September 2020

1.0 Aims

1.1 To ensure the safety of all students and staff while working online.

2.0 Authorised Access

2.1 Internet access for pupils should be seen as an entitlement on the basis of educational need and an essential resource for staff.

2.2 The School receives Internet Service Provision (ISP) from INFONAS and has a separate filtering service from SmoothWall which proactively monitors Internet usage for attempts to access illegal and immoral content.

2.3 The School actively monitor both systems and will notify the Head of School, which can be referred to the local police in these instances.

2.4 The School receives filtering from SmoothWall and can request monitoring reports based on information setup from the Head of IT which will be regularly checked to identify any attempts to access illegal content and should notify the Head of School.

2.5 E-mails are monitored and filtered via Google Suite

2.6 The School will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date; for instance, if a pupil's access is withdrawn.

2.7 ALL students must apply for Internet access individually by agreeing to abide by the Acceptable User Policy statement that is signed in conjunction with their parents at the point of registering with the School together with the School Rules

2.8 The pupils will receive an annual reminder regarding the School's AUP.

3.0 Filtering and Monitoring

3.1 Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content. Levels of access and supervision vary according to the pupil's age and experience. Internet access must be appropriate for all members of the school community from the youngest pupil to staff.

3.2 A log of all staff with varying levels of access to the internet will be kept and regularly reviewed.

3.3 The Head of IT, working in conjunction with the Heads of School will review the popular permitted and banned sites accessed by the School.

3.4 The School will work in partnership with parents, its ISP to ensure systems to protect pupils are reviewed and improved.

3.5 If staff or pupils discover unsuitable sites, the URL (web address) and content must be reported to the ICT Department, which will then be blocked.

3.6 Website logs and internet usage are screened, and a weekly report created for the attention of The DSLs.

3.7 Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.8 Any material that the School believes is illegal or may place an individual at risk must be referred to the appropriate authorities i.e. Head of School, DSL, Police, etc

4.0 Risk Assessment

4.1 As the quantity and breadth of the information available through the internet continues to grow, it is not possible to guard against every undesirable situation. The School addresses the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the school system.

4.2 In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. The School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The School cannot accept liability for the material accessed or any consequences of Internet access.

4.3 Methods to identify, assess and minimise risks will be reviewed regularly.

4.4 The Senior Leadership Team will ensure that relevant Policies is implemented and compliant with the policy monitored.

4.5 The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence

5.0 Teaching and Learning

With the explosion in technology, the School recognises that blocking and barring sites is no longer adequate. The BSB teaches all of its pupils to understand why they need to behave responsibly if they are to protect themselves. This aspect is a role for each School's Designated Safeguarding Lead, PSHE Co-ordinators, HOY and Pastoral staff.

5.1 The Curriculum

5.1.1 Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

5.1.2 The purpose of Internet use in School is to raise educational standards, to promote pupil achievement, ensure wellbeing, to support the professional work of staff and to enhance the School's management information and business administration systems.

5.1.3 Whilst Internet access is an entitlement, users will need to show a responsible and mature approach to its use or this privilege may be removed.

5.1.4 The Internet is an essential part of everyday life for education, business and social interaction. The School has a duty to provide students with quality Internet access as part of their learning experience.

5.1.5 Pupils use the internet widely outside School and need to learn how to evaluate Internet information and to take care of their own safety and security.

5.2 Evaluating Content

5.2.1 Information received via the internet, e-mail or text message requires good information-handling and digital literacy skills. In particular, it may be difficult to determine origin and accuracy, as the contextual clues may be missing or difficult to read.

5.2.2 Ideally inappropriate material would not be visible to pupils using the internet but this is not easy to achieve and cannot be guaranteed.

5.2.3 Pupils will be taught through PSHE and Computing lessons what to do if they experience material that they find distasteful, uncomfortable or threatening.

6.0 Communication and Content

6.1 Managing e-mail

6.1.1 E-mail is an essential means of communication for both staff and pupils. The School's current e-mail provision is Google Suite. The following safety measures should be adhered to:

6.1.2 Pupils may only use approved e-mail accounts on the school system, unless otherwise directed by a member of staff.

6.1.3 Pupils may NOT send an e-mail to ALL pupils.

6.1.4 Pupils must immediately tell a responsible adult if they receive offensive e-mail.

6.1.5 Staff must use official School provided e-mail accounts for all professional communications.

6.1.6 Pupils should use e-mail in an acceptable way. Sending images without consent, explicit images, messages that cause distress and harassment to others are considered significant breaches of school AUP and will be dealt with accordingly.

6.1.7 E-mail sent to an external organisation should be written carefully and where appropriate, authorised before sending, in the same way as a letter written on School headed paper.

6.2 Online communications and Social Media.

6.2.1 Online communications, social networking and social media services may be filtered in School by SmoothWall when using the School's network, but are likely to be accessible on their own devices or from home.

6.2.2 E-mails are monitored and filtered by Google Suite.

6.2.3 All staff are made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They are aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

6.2.4 Pupils are encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

6.2.5 The School has a key role to teach young people about the importance of how to communicate safely and respectfully online, keeping personal information private.

6.2.6 Users will be taught about how to keep personal information safe when using online services. Examples would include real name, address, mobile or landline phone numbers, School attended, and e-mail addresses, full names of friends/family, specific interests and clubs etc.

6.2.7 Users must not reveal personal details of themselves or others in online communication, including the tagging of photos or video, or to arrange to meet anyone.

6.2.8 Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the site's terms and conditions to ensure the site is age-appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.

6.2.9 Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the School where possible.

6.2.10 Pupils will be advised on security and privacy online, and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.

6.2.11 Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.

6.2.12 No member of the school community should publish specific and detailed private thoughts about the School, especially those that may be considered threatening, hurtful or defamatory.

6.2.13 No member of the school community should engage in behaviour on social media sites that may be considered detrimental to the School and its reputation.

6.2.14 Parents wishing to photograph or video at an event should be made aware of the school's expectations and be required to comply with the schools AUP as a condition of permission to photograph or record.

6.2.15 Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of School) will be raised with their parents/carers, particularly when concerning students' underage use of sites.

6.2.16 Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction, and safe and professional behaviour will be outlined in the School Acceptable Use Policy.

6.2.17 It will not be considered appropriate for staff to engage in personal online communications with children and young people, parents or carers.

6.2.18 Express care is also to be taken regarding the use of social networking sites.

6.3 Mobile Devices (Including Bring Your Own Device-BYOD)

6.3.1 Pupils are discouraged from bringing expensive items such as phones into School. However, to enable any essential family communication, a mobile phone is accepted under the following conditions:

6.3.2 it is the responsibility of the pupil to keep it safe o

6.3.3 it is NOT to be used as a timekeeper or calculator

6.3.4 it is turned off and out of sight during the school day between 0720 - 1515.

6.3.5 Video/Camera-phones may only be used on school trips with the express permission of the trip organiser. If phones are being used to take photographs, normal school rules and expectations would apply.

6.3.6 School staff authorised by the Head of each School may search pupils or their possessions and confiscate any mobile device they believe is being used to contravene school policy, constitute a prohibited item, is considered harmful, or detrimental to school discipline.

6.3.7 If it is suspected that the material contained on the mobile device relates to a criminal offence, the device will be handed over to the police for investigation.

6.3.8 Sending abusive or inappropriate messages or content over social media platforms is forbidden by any user within the school community.

6.3.9 School staff may request a pupil reveal a message or show them other content on their phone for the purpose of establishing if a contravention of the school rules is suspected.

6.3.10 With the pupil present a member of the SLT may search through the phone in a case where they are reasonably suspected of involvement in an activity that contravenes the school rules.

6.3.11 Mobile devices may be used during lessons or formal school time as part of an approved and directed curriculum-based activity.

6.3.12 Mobile devices are NOT permitted to be used in certain areas or situations within the school site, e.g. changing rooms or toilets, situations of emotional distress etc.

6.3.13 Where staff may need to contact children, young people and their families within or outside of the setting in a professional capacity, they should only do so via an approved school account (e.g. e-mail, phone, social media) In exceptional circumstances, there may be a need to use their own personal devices and account; this should be notified to a senior member of staff ASAP.

6.3.14 Staff should be provided with school equipment for taking photos or videos of pupils linked to an educational intention. Staff MUST NOT use personal devices for such a purpose.

6.3.15 The School will take steps to monitor responsible use in accordance with the Acceptable Use Policy.

6.4 Video Conferencing guidelines

6.4.1 Please refer to the Remote Learning Policy for further detail

6.4.2 All teachers are encouraged to conference call individual pupils and small groups to check in, catch up and facilitate instructions and discussions.

6.4.3 If delivering lessons from home, all should be aware of the material that may be visible in the background.

6.4.4 All participants should avoid revealing personal teacher information or other sensitive data.

6.4.5 All pupils and teachers that can be seen during a remote learning lesson should also be properly dressed and in a suitable, public location (such as a kitchen or living room) and not in a bedroom.

6.4.6 Video calls to one pupil should not be made unless a parent/guardian is present or is aware of the call. Exceptions to this include:

6.4.6.1 What would normally be 1:1 e.g. SEN, Music, Drama, TA support or classes of one pupil

6.4.6.2 VMTs

6.4.7 Photographs of individuals (staff or other pupils) are personal data; therefore, screenshots of other members of the online learning environment cannot be taken and cannot be used unless consent is given.

6.4.8 All lessons and calls must be recorded and all participants should be made aware.

6.4.9 All teachers delivering online lessons should log out at the end of the session.

7.0 GDPR and data security:

7.1 This advice pertains to all users when remote learning:

7.1.1 Ensure computers are stored securely, out of view and shut down every night.

7.1.2 Keep anti-virus software up to date.

7.1.3 Install latest software updates promptly.

7.1.4 Close laptop lids when temporarily not in use as webcams may stay on without a user realising.

7.1.5 If others are in the room, protect any sensitive data that you might have on your screen.

7.1.6 Ensure your passwords are strong and only known by you.

7.1.7 Beware of scams – fraudsters have been quick to take advantage of the latest crisis

8.0 Emerging Technologies

8.1 Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools.

8.2 Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in School is allowed.

9.0 Cyber Bullying

9.1 Cyber bullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet, to deliberately hurt or upset someone" DCSF 2007.

9.2 For most, using the internet and mobile devices is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively.

9.3 The school endeavours to ensure that young people, school staff, parents and carers understand the similarities and differences between cyber bullying and other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users supports innovation and safety.

9.4 Cyber bullying (along with all other forms of bullying) of or by any member of the school community will not be tolerated.

9.5 Full details are set out in the School's Behaviour, Anti-Bullying and Child Protection Policies, which include:

9.6 Clear procedures set out to investigate incidents or allegations of cyber bullying.

9.7 Clear procedures in place to support anyone in the school community affected by cyber bullying.

9.8 All incidents of cyber bullying reported to the School will be recorded.

9.9 The School will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting SmoothWall and the police, if necessary.

9.10 Pupils, staff and parents/carers will be required to work with the School to support the approach to cyber bullying and the School's e-Safety ethos.

9.11 The School expects pupils to treat staff and each other online with the same standards of consideration and good manners as they would in the course of face-to-face. They should always follow the School's Rules and Regulations.

9.12 Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated.

9.13 The School is strongly committed to promoting equal opportunities for all, regardless of race, gender, gender orientation or physical disability.

9.14 All pupils are encouraged to look after each other and to report any concerns about the misuse of technology or worrying issue to a member of the pastoral staff.

10.0 Implementation

10.1 Policy in Practice Pupils

10.1.1 Many pupils are very familiar with Internet use and the culture that surrounds it.

10.1.2 The School's e-safety teaching and awareness-raising is important in discussing the key features with pupils as appropriate for their age.

10.1.3 Pupils are reminded of the school rules at the point of Internet use.

10.1.4 All users will be informed that network and Internet use will be monitored.

10.1.5 Online Safety teaching should be integral to the curriculum and raise the awareness and importance of safe and responsible internet use amongst pupils.

10.1.6 Online Safety teaching will be included in PSHE and/or ICT and cover safe use at School and home.

10.1.7 Online Safety rules and/or copies of the Acceptable User Policy

10.1.8 Safe and responsible use of the internet and technology will be reinforced across the curriculum and subject areas.

10.2 Policy in Practice – Staff

10.2.1 The Online Safety Policy will be provided to and discussed with all members of staff and Acceptable User Policy signed for compliance.

10.2.2 Staff should be aware that Internet traffic is monitored and can be traced to the individual user.

10.2.3 Discretion and professional conduct are essential.

10.2.4 Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.

10.2.5 All members of staff will be made aware that their online conduct out of School could have an impact on their role and reputation within School.

10.2.6 Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

10.3 Policy in Practice - Parents

10.3.1 Parents need to be aware of the potential dangers that are associated with online communications, social networking sites and mobile technologies to help ensure their children are not putting themselves at risk.

10.3.2 The School will always contact the parents if it has any concerns about pupils' behaviour with regards to e-safety and likewise it hopes that parents and guardians will be able to share any concerns with the School.

10.3.3 Parents' attention will be drawn to the Online Safety Policy and Acceptable User Policy (AUP)

10.3.4 A partnership approach with parents will be encouraged. This will include offering parent evenings, demonstrations, practical sessions and suggestions for resources and safer Internet use at home.

10.3.5 Regular information will be provided to parents about how to ensure they can work with the School to ensure this resource is used appropriately both within School and home.

10.3.6 Internet issues will be handled sensitively to inform parents without undue alarm.

11.0 Handling of complaints

11.1 Responsibility for handling incidents will be delegated to a senior member of staff.

11.2 Any complaint about staff misuse must be referred to the Executive Headmaster.

11.3 Pupils and parents will be informed of the complaints procedure.

11.4 Parents and pupils will need to work in partnership with staff to resolve issues.

11.5 There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.