BRITISH INTERNATIONAL SCHOOL

Dare to Dream

Online Safety Policy

AIMS OF THIS POLICY

The aim of this Online Safety Policy is to ensure that students, staff, parents and visitors benefit from opportunities offered by school's Internet and IT Systems in a safe and effective manner. The school aims to ensure that all people using these systems do so responsibly and with good judgement so that uninterrupted, safe and appropriate access can continue throughout the school.

All members of our school community have the right to be free of any fear of cyber bullying by anyone known or unknown. We should be able to recognise cyber bullying and be fully equipped to be able to deal with it effectively should they encounter it, as well as fully understanding how to use the internet safely and effectively.

In line with our School Vision and Mission, this policy aims to ensure that our students, staff, parents and visitors help to empower our students to be happy, innovative leaders who understand and embrace global citizenship and who are equipped for a fast-changing future. This policy aims to uphold and promote the School Values of Integrity, Responsibility, Empathy and Peace.

SCOPE OF THIS POLICY

This policy applies to all students, staff (academic and administrative) parents and visitors to the school who function online for the purposes of school activities and are granted access to the Internet or IT Systems. This policy covers use from both with the school and through remote access.

This policy addresses:

- Roles and Responsibilities of the Online Safety Group
- Reporting and Managing Online Safety Incidents
- Strategies for Managing Unacceptable Use
- Online Safety Education
- Managing Digital Content and Social Media
- General Guidelines in Support of Online Safety
- The School's IT Infrastructure

This policy links with the following policies and guidelines:

- BIS Acceptable Use Policy for Students
- BIS Acceptable Use Policy for Staff
- BIS Online Safety Education Curriculum
- BIS Managing Digital Content and Social Media Policy
- UAE Laws on Labour, Cyber Crimes and Child Protection

LEGAL UNDERTAKING

The British International School, Ajman is committed to supporting and complying with all Federal Laws of the UAE related to Cyber Crimes and Child Protection which give clear guidelines on what is and is not acceptable. The school is committed to protecting all children in its care by monitoring all online activities, taking action on any violations, reporting any crimes to the relevant authorities and providing training and awareness to all students.

ROLES AND RESPONSIBILITIES OF THE ONLINE SAFETY GROUP

Whole-Group Responsibilities:

- Develop, Monitor and review all e-safety, online and relevant IT policies and procedures
- Monitor the online e-safety incident record (managed by the Student Wellbeing Team)
- Be made aware of any incidents that may occur and work with the Student Wellbeing Team to help decide on any actions required where necessary
- Monitor any issues that may arise and be up to date with changes and developments in technology that may, in particular, have an impact on student safeguarding (eg new apps, changes in security permissions)
- Discuss and decide on training and awareness programmes for various members of the school community, develop and deliver the programmes and review them through feedback from the participants
- Oversee the development of an ongoing broad e-safety curriculum, its development, implementation and review of its effectiveness
- Oversee all activities and programmses offered with the goal of promoting e-safety

Online Safety Leader:

- Chair all meetings (which should be held twice per term), ensure that minutes are taken outlining agenda items to be discussed and actions required recorded
- Ensure that all action points from meetings are followed up and provide support where required
- Share minutes and other relevant documentation with key stakeholders (school leaders etc

Senior Leadership Representative/s:

- Ensure that all decisions, policies and practices initiated by the group are in line with the whole school policies and strategic direction and are addressing the schools guiding statements
- Brief SLT members and other relevant stakeholders of the group's activities

Student Wellbeing Representative/s:

- Work with outside agencies as required on issues of e-safety and child protection in relation to technology
- Maintain the E-safety Incident Register (included as part of the general Behaviour Management Register) and ensure that any e-safety issues are addressed accordingly

ICT Teachers:

- Develop a broad E-Safety Curriculum that can be delivered in ICT classes, ensuring that it is in line with the school's ICT curriculum and working with the Student Wellbeing Team ensuring all appropriate points are covered
- Keep up to date with developments and changes in technology and to inform the group of any relevant information such as new apps and programs, changes in app security settings, general online trends etc

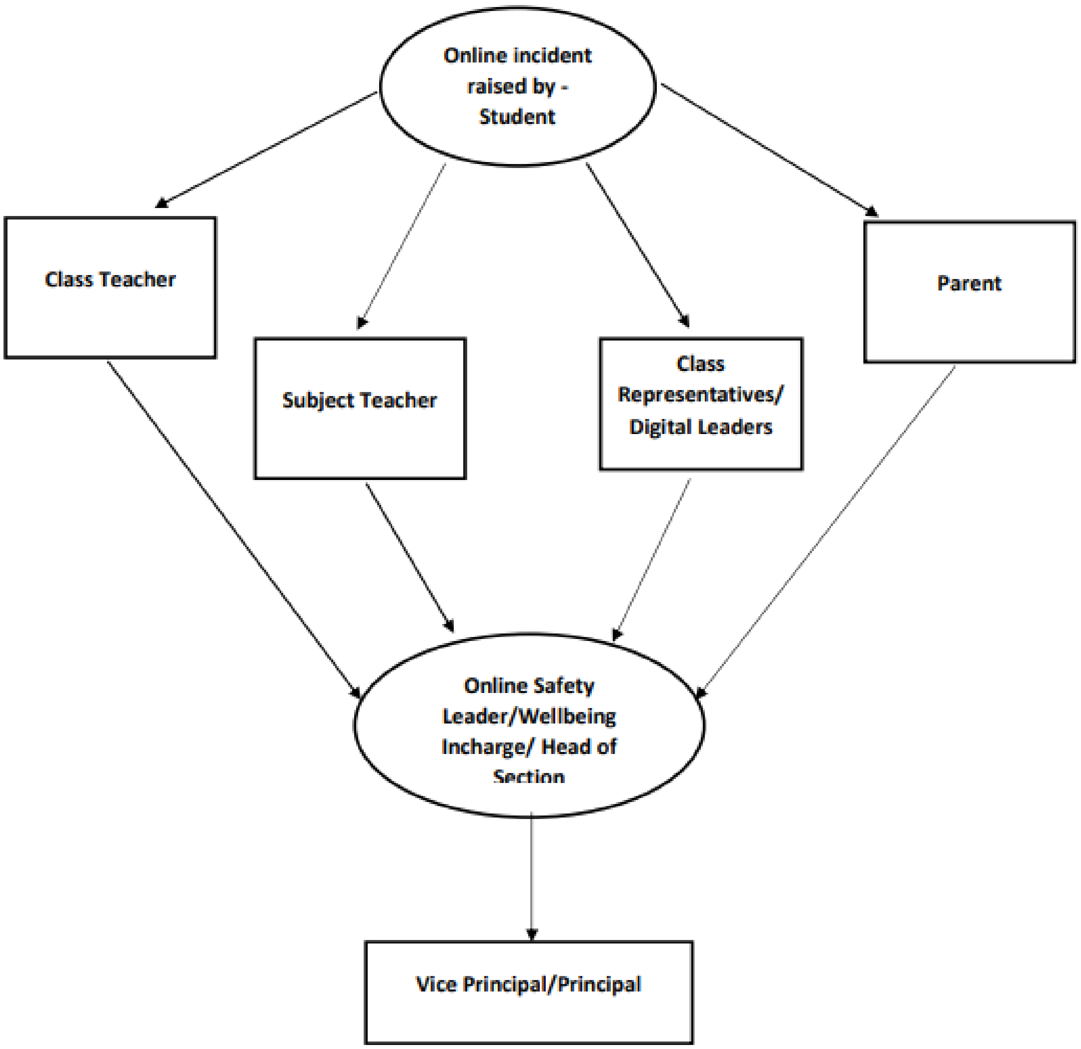
IT Support Staff:

- Provide updates on any network issues, security concerns or other potential threats that may impact student safeguarding
- Provide advice on usage of filtering to ensure age-appropriate filtering is in place
- Advise on any other relevant IT issues that may impact student safeguarding

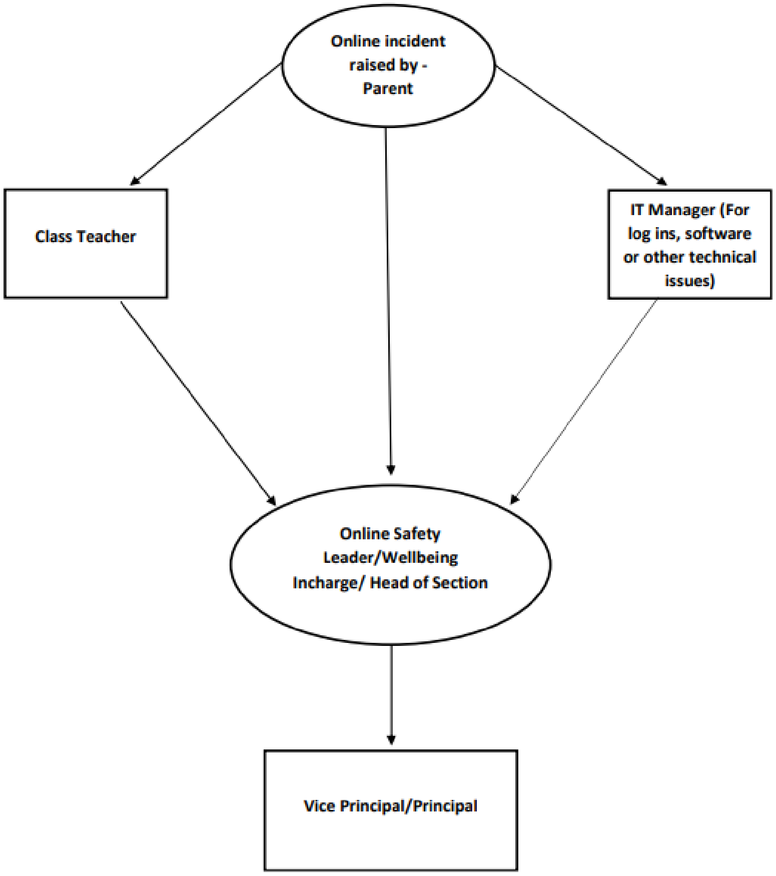
REPORTING OF AND MANAGING ONLINE SAFETY INCIDENTS

The school has developed a comprehensive system for the reporting of online safety incidents including the strategies for managing unacceptable use as detailed below. All members of the school community can report any incident through a number of channels as outlined below:

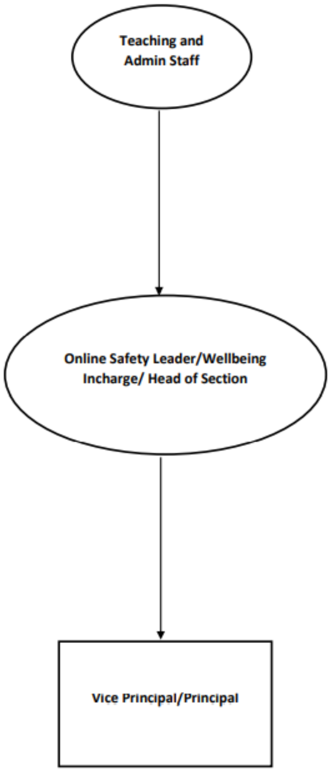
Reporting Online Incidents Flowchart for Students


Online incident raised by - Student
Class Teacher
Subject Teacher
Class Representatives/ Digital Leaders
Parent
Online Safety Leader/Wellbeing Incharge/ Head of Section
Vice Principal/Principal

Reporting Flowchart for Parents


Online incident raised by - Parent
Class Teacher
IT Manager (For log ins, software or other technical issues)
Online Safety Leader/Wellbeing Incharge/ Head of Section
Vice Principal/Principal

Reporting Flowchart for Staff



Communication Channels and Methods for Reporting Online Safety Incidents

Students *-can report to:*	**Class Digital Leaders** *-can report to:*	**Parents** *-can report to:*	**Teaching and Admin Staff** *-can report to:*
-Class teachers -Subject teachers • Through email, verbal complaint, online form uploaded on homeroom teams -Class Digital leaders • Through student connect council, verbally on individual basis -Counsellor • Can approach anytime through email, verbal complaint.	-Online Safety Leader -Wellbeing In charge -Head of Section • Through online form uploaded on Student Council Members (separate girls and boys), Verbal complaint to Head Girl -Counsellor • Can approach anytime through email, verbal complaint.	-Class teacher -Online Safety Leader • Through email • Phone call to Reception -Wellbeing In charge -Head of Section • Through email/Hotline numbers -Principal/Vice Principal • Through email IT/Technical/E-Safety Issues –Contact the IT manager for any issues arising with log ins, software or other technical elements during the distance learning period. If any other person will be contacted, they will also forward the concern to IT Manager.	*<u>Teaching Staff</u>* -Online Safety Leader -Wellbeing In charge -Head of section • Through online form, email. *(Evidence should be attached)* *<u>Admin Staff</u>* -Online Safety leader -Wellbeing In charge -Head of section • Through online form, email. *(Evidence should be attached (If any))* -Counsellor • Can approach anytime through email, verbal complaint.

STRATEGIES FOR MANAGING UNACCEPTABLE USE

The main areas of risk for our school community are as follows:

Content

- Exposure to inappropriate content (e.g. violence, language, sexualised content)
- Lifestyle websites promoting harmful behaviours (e.g. body shaming, intense dieting programmes)
- Hate content (e.g. bullying, racism, extremism, discrimination)

Contact

- Grooming (e.g. sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Privacy issues, including disclosure of personal information

- Digital footprint and online reputation
- Health and well-being (e.g. amount of time spent online)
- Sexting
- Copyright (e.g. little care or consideration for intellectual property and ownership)

Guidance: What do we do if…?

An inappropriate website is accessed unintentionally in school by a teacher or student

- Remain calm
- Report to the online safety leader/wellbeing in charge/Head of Sections and decide mutually decide whether to inform parents of any children who viewed the site.
- Inform the school technicians/IT Manager and ensure the site is blocked

An inappropriate website is accessed intentionally by a student

- Ensure all evidence is stored and logged
- Refer to the Acceptable Use Agareement that was signed by the student and apply agreed sanctions (MOE Behavioural policy, dealing with online safety incidents)
- Notify the parents of the student
- Inform the school technicians and ensure the site is blocked

An inappropriate website is accessed intentionally by a staff member

- Refer to Head of Section.
- Head of Section ensures that all evidence is stored and logged and report to Vice Principal/Principal
- Refer to the Acceptable Use Agreement that was signed by the staff member, and apply disciplinary procedures
- Inform the school technicians and ensure the site is blocked
- In an extreme case where the material is of an illegal nature, the School Principal or their nominee must contact the police and assist in their investigations

An adult uses School IT equipment inappropriately.

- Report the misuse immediately to the head of Section
- Head of Section ensures that there is no further access to the device and to record all actions taken
- If the material is offensive but not illegal, the head of section should then:
  - Remove the device to a secure place
  - Instigate an audit of all ICT equipment by the school's ICT technical teams to ensure there is no risk of students accessing inappropriate materials in the school
  - Identify the precise details of the material
  - Inform Vice Principal/Principal and take appropriate disciplinary action

In an extreme case where the material is of an illegal nature:

- The School Principal or their nominee must contact the police and assist in their investigations
- If requested, remove the device to a secure place and document what actions have been taken

All of the above incidences must be reported (even after resolving) to the Online Safety Leader and the School Principal.

A bullying incident directed at a student occurs through email or mobile phone technology, either inside or outside of school time:

- Advise the student not to respond to the message
- Secure and preserve any evidence through screenshots and printouts
- Refer to relevant policies including online safety anti-bullying and apply appropriate sanctions
- Notify parents of all the children involved
- Consider delivering a parent workshop for the school community

- The School Principal or their nominee should contact the police and assist in their investigations where necessary
- The School Principal or their nominee should contact other agencies if necessary (Child protection, police liaison officer)

Malicious or threatening comments are posted on an Internet site (such as social media) about member of the school community (including students and staff).

- Secure and preserve any evidence through screenshots and printouts
- Inform and request the comments be removed if the site is administered externally
- Send all the evidence to a suitable senior staff member (Section Head, Online Safety Leader etc)
- The School Principal or their nominee should contact the police and assist in their investigations where necessary
- The School Principal or their nominee should contact other agencies if necessary (Child protection, police liaison officer)

Concern about a student's safety being at risk because of suspicion they are playing online games that are inappropriate or certificated beyond the age of the student

- Report to online safety leader/wellbeing incharges/head of sections
- Advise the student and their parents on appropriate games and content.
- If the game is played within school environment, ensure that the technical team block access to the game
- The School Principal or their nominee should contact the police and assist in their investigations where necessary
- The School Principal or their nominee should contact other agencies if necessary (Child protection, police liaison officer)
- Consider delivering a parent workshop for the school community, if required.

You are aware of social network posts and pages created by parents about the school. Whether information is accurate or inaccurate, the posts are inflammatory and disruptive to the school community:

- Report to online safety leader/wellbeing in charges/head of sections/vice Principal/Principal
- Contact the poster or page creator and discuss the issues in person
- Ensure staff training outlining how to respond when finding such posts and appropriate responses
- Contact governing body and parent association, if needed
- Consider delivering a parent workshop for the school community, if required
- Consider any legal action after all other avenues to resolve the situation have been exhausted. The School Principal or their nominee should contact the police and assist in their investigations where necessary

ADVICE FOR PARENTS IF ANONLINE SAFETY INCIDENT DOES OCCUR

When an online safety incident occurs, school staff will work through an incident response procedure, which is underpinned by school policies and guidelines from the Ministry of Education. Please contact the school for a copy of the policies and procedures if you do not have them and familiarise yourself with the response steps.

Focus on wellbeing

- Check in regularly with your child and the contact person at your school. Regardless of whether your child was the target, instigator or bystander in the incident, it is likely that they will require emotional support. If your child has used technology inappropriately, support them to take responsibility for their actions and give them ideas to resolve the issue.
- Seek professional help if your child is distressed or shows changes in behaviour or moods. Maintain contact with the school so you can work together to support your child.

Communicate with the school

- Make a list of questions that you want to discuss with the school and use this to guide conversation. Check if your child has questions as well, or if they have any ideas on how to resolve the issue or repair the harm.
- Throughout the process it is important that communications with the school are calm and positive, focusing on addressing the issues and supporting your child. You might like to ask the school to watch out for concerning behaviours, or discuss the strategies that will be implemented if the issue remains unresolved.
- Keep in regular contact with the school, making set times to meet with your child's teacher, school counsellor and, if needed, the principal or school wellbeing team. This may help support the wellbeing of your child particularly if you have concerns with the steps taken in managing the issue, or if your child starts to feel uncomfortable about attending school.

Access support

- The school can provide support. There are also a range of external agencies that may be of assistance. The school can provide some suggestions on organisations that can offer counselling and support services that can help anyone involved in an online safety incident.

Be Informed

- A number of websites offer a range of information for Parents including skills and advice to help you talk to your child about online safety issues including cyberbullying, inappropriate material and online gaming. Please ask the school for assistance if required.

ONLINE SAFETY EDUCATION

Students

The education of students in online safety is an essential part of the school’s online safety provision. Our students need to understand the potential hazards they may encounter online and they need the help and support of school to recognise and avoid online safety risks and build their resilience, supported by informed parents.

Online safety is a focus in all areas of the curriculum and staff are expected to reinforce online safety messages across the curriculum. The school’s online safety curriculum is a broad but comprehensive programme that provides progression and development of knowledge and skills throughout the grade levels with topics that are age appropriate. The school has chosen to base its online safety education programme around the “Education for a Connected World – 2020 Edition” framework published by the UK Council of Internet Safety. This framework is current and up to date and comprehensively covers all aspects of online safety to ensure a well-rounded education for our students.

The Online Safety Education programme will be delivered through:

- The planned online safety curriculum will be provided as regular stand-alone lessons throughout the year on a regular ongoing basis
- Some lessons will be delivered as part of the ICT classes
- Key online safety messages should be reinforced as part of the planned programme of assemblies and wellbeing activities
- Students will be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students will be guided to understand the need for the Acceptable Use Policy for Students and encouraged to adopt safe and responsible use both within and outside school
- Staff are expected to model best practice in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, students will 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 are expected to be vigilant in monitoring the content of the websites the students access
- The school acknowledges that, from time to time, and for sound educational reasons which are linked to the delivery of the curriculum, students (mainly senior) may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In these cases, teachers can request approval from the Principal through their HOD to have specific sites temporarily unblocked for a set period of time. Any request of this nature will be recorded and kept with the auditing records of the school's filtering provision.

Teachers and Staff
It is essential that all school staff receive suitable online safety training and understand their responsibilities, as outlined in this policy.
Training will be offered as follows:

- A programme of formal online safety training will be delivered to staff, including non-teaching staff. An audit of the online safety training needs of all staff will be carried out regularly and the programme of training will be updted based on the audit, staff surveys and developing technologies accordingly.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school's Online Safety Policy, Acceptable Use Policy for Staff and all other policies and procedures related to online safety.
- The Online Safety Leader will attend external training and workshops to ensure their knowledge is current. They are expected to share this knowledge through suitable training sessions for staff
- This Online Safety Policy, related policies and practices will be referenced in staff meetings and professional development sessions on an ongoing basis throughout the school year
- The Online Safety Leader will be available to all staff to provide any individual guidance on aspects of Online Safety as and when required

Parents and the Wider Community
The school acknowledges that parents may not have as well-developed an understanding of online safety as is required for providing their children with the required support at home. Therefore, the school will help to ensure that parents are informed of online safety through the following means:

- Letters / circulars discussing various aspects of online safety
- Sharing of all relevant school policies related to online safety through email and access on the school website
- Dedicated online or, where possible, in-person information sessions related to online safety including videos and links to suitable websites
- Awareness campaigns such as IT Month, Safer Internet Day
- Engaging with other community organisations where appropriate to promote online safety

MANAGING DIGITAL CONTENT AND SOCIAL MEDIA

The school is committed to managing digital content and social media in a way that ensures safety and privacy for all members of the school community. Full details are available in the ***BIS Managing Digital Content and Social Media Policy***.

To help ensure that digital content is managed effectively, the following strategies are included in the policy:

- Staff will educate students on the appropriate use of images and videos of themselves and others, especially concerning publishing on social media
- Parents can take images and videos of their children during school activities for their own personal use but must not publish or distribute them
- Staff can take images and videos of student for school purposes using school equipment and should not publish or distribute them

- Permission must be gained from parents before using any images of students along with samples of student work in school social media
- Students must not take, use, share, publish or distribute images of others without their permission
- School staff are expected to exercise professionalism when using social media for personal use, including careful consideration of all content published and comments made on any social media site either related or unrelated to the school
- Teachers are expected to use the school sanctioned platforms only to communicate with students and parents and to do so in an appropriate and professional manner at all times

GENERAL GUIDELINES IN SUPPORT OF ONLINE SAFETY

Internet Access

- Internet usage at school by all students and staff will be regularly and strictly monitored
- When at school, Internet will only be used by students and staff for e-learning purposes, file sharing and collaborative work
- School will provide support and training to all staff about online safety to ensure they are able to protect themselves and students from the potential risks of using the Internet and also to deal with online incidents should any occur
- All systems will be installed with updated anti-virus software to limit spread of any malicious software
- All systems will have safe-search settings set to minimize the risk of exposure to inappropriate content
- All Internet sessions held at school will always be under teacher supervision
- Uploading and downloading of unauthorised softwares are strictly prohibited
- Use of pen-drives/USBs or any other storage media is only allowed with teacher’s permission and after it is scanned for viruses and other malicious software
- School IT staff has access to all files used on school systems and portals, including e-mails exchanged by students to discourage use of offensive mails and content

Web Browsing

- All students should be critically aware of the content they access online, whether at school or outside of school
- Web browsers at school should only be used for educational purposes of research and information gathering from various websites and databases
- All students and staff are aware of copyright issues pertaining to online materials. New students and staff are provided with relevant training as and when they join
- Any internet usage including sites and downloads may be monitored for unusual activity or for security and network management reasons and be blocked by school if the school considers them unsuitable or they are thought to be damaging to the school community

E-mail Accounts

- Students must only use approved school e-mail accounts for e-learning purposes
- Students must keep their allocated username and password confidential and not share it with anyone. If the credentials are compromised intentionally or unintentionally and is identified by the IT staff, the e-mail account will be disabled promptly for security purposes
- No student is allowed to access or change any other person’s username, password, files or data
- E-mails should only be exchanged with known people and who are approved by teachers or parents

School Online Platform

- All students have access to MS Teams for attending online lessons, file sharing and collaborative work
- Use of any other platform is allowed only if it is approved by the school and all forums are always supervised
- Students are not allowed to use MS Teams for any personal reasons. If any unauthorised activity is identified, student account will be disabled temporarily

- Students should not mock others during the online meeting, through chats or calls on MS Teams
- Restricted access rights are given to students using MS Teams for e-learning – they cannot remove anyone from an on-going meeting, mute others, cause any disturbance to the presenter and other attendees
- Sharing of unauthorised content on MS Teams is strongly discouraged. Failure to abide by this will result in strict consequences

Expectation of Parents

To help ensure that all students in our school community are safe online, we ask parents support through the following ways:

- Monitor and enforce their own family values to their children making them aware of the importance of using Internet safely
- Involve their children in regular discussions regarding the different challenges that are presented through the Internet
- Ensure that the children are aware of the acceptable Internet discipline and the consequences if the rules are broken
- Maintain clarity and consistency on what is permissible and what activities are unacceptable
- Assume complete responsibility for monitoring their children's use of Internet at home and outside school
- Have complete awareness of cyber bullying and ensure that the children are not being subjected to it in any form through monitoring and discussions
- Inform and work with the school if any misuse is reported or found
- Seek help and support from the school in case of any incident that involves cyber bullying
- Be well informed about the work or projects given to the children to rule out any misuse. In case of any concerns they should check with the school immediately

THE SCHOOL'S IT INFRASTRUCTURE

The school is be responsible for ensuring that the school infrastructure / network is as safe and secure as possible and that guidelines in this policy are implemented. The school also ensure that the relevant people within the school undertake their duties so that:

- School technical systems are managed in ways that ensure that the school meets fundamental technical requirements
- An audit process of the safety and security of school technical systems is in place to monitor and review effectiveness of the systems
- All server / switch systems are in locked, AC-cooled rooms with restricted access
- All users have clearly defined access rights to school technical systems and devices
- Internet access is filtered for all users and monitored regularly. This is acknowledged through the Acceptable Use Polices and Agreements
- An appropriate system is in place (to be described) for users to report any actual / potential technical incident / security breach to the relevant person, as agreed)
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices 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
- An agreed policy is in place for the provision of temporary access of visitors onto the school systems

PASSWORD SECURITY

Password Creation

- Students should create a password that is easy to remember for them but difficult for others to figure out. Students should not use their name, date of birth, parents name etc. but a combination of words and numbers that are uniquely memorable for the student.
- Teachers should create a password that is also a balance between being memorable but not easily figured out by others. Teachers are encouraged to have different passwords for different accounts, especially being different for school accounts compared to personal accounts.
- Senior Leaders and Administration Staff should create unique passwords that are difficult for anyone to be figured out and should be kept secure due to the sensitivity of the data in various systems.

Password Change

- For students, School IT systems will provide an automatic Password Change facility once every 6 months
- On other occasions, students should change passwords only when there is reason to believe a password has been compromised.
- If students need help to change their password, they should approach the IT Department.
- For teachers, School IT systems will provide an automatic Password Change facility once every 6 months
- Teachers should change passwords whenever it is suspected that it has been compromised.
- For Senior Leaders and Admin staff who access sensitive information, School IT systems will provide an automatic Password Change facility once every 90 days
- Senior Leaders and Admin staff must change their password immediately if it is suspected that it has been compromised

Password Protection

- The school IT Systems have Password Recovery facilities for all users
- School IT Systems force password strength on creation and renewal through minimum complexity requirements including minimum 8 characters requiring alpha and numeric, upper and lower case
- Passwords must not have the username as part of the password
- Students must not share their passwords with anyone including other students, teachers, friends or relatives. However, they should be prepared to share their passwords with their parents only.
- Students should not write or store their passwords anywhere, especially in class note books and other materials they carry with them.
- Teachers and Administration staff should not share their passwords with anyone. This is particularly important that teachers do not share their passwords with students if they have forgotten their own.
- All teachers and students must not use the "Remember Password" feature of applications (for example, web browsers).
- Any teacher, administrative staff or student suspecting that their password may have been compromised must report the incident to IT or Senior Leadership and change all passwords as soon as possible.

FILTERING

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use of the Internet and IT Systems.

The responsibility for the management of the school's filtering will be held by the IT Staff and overseen by the School Principal. They will manage the school filtering in line with this policy and IT Staff will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service:

- must be logged
- must be reported to the Principal
- must be reported to the Online Safety Group regularly in the form of an audit of all data logged

All users have a responsibility to report immediately to IT Manager any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice:

- The school maintains and supports the managed filtering service
- The school has provided enhanced / differentiated user-level filtering through the use of firewall and individual monitoring, blocking requests
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is approved by the Principal
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems
- Any filtering issues should be reported immediately to the IT Staff
- Requests from staff for sites to be blocked or unblocked for any reason from the filtered list will be considered by the technical staff and only actioned after permission of the Principal is granted. When the request is made and permission is given, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.

Auditing and Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- The school Principal in a weekly IT Infrastructure report
- Online Safety Leader and Online Safety Group in monthly meetings
- Senior Leadership Team and Online Safety Group through a once-termly full auditing process
- Government authorities if / when necessary

TECHNICAL SECURITY

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access
- No user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- Access to personal data is securely controlled in line with the school's Data Protection Policy
- Logs are maintained of access by users and of their actions while users of the system

- There is effective guidance and training for users
- There is oversight from senior leaders and these have impact on policy and practice.
- There school operates a central filtering system
- The system can also be deployed at school level if required, but the standard configuration has distinct filtering levels for staff and pupils.
- Filtering change requests are online and are only accepted from authorised users. Any changes are security checked before implementation.
- The system provides full monitoring and reporting. These reports are available to the relevant authorities when requested

The school provides:

- Email anti-spam
- Secure email facilities
- Full anti-virus
- Encrypted document exchange
- Remote access authentication
- Industry standard firewalls to protect both WAN and school LANs
- IT Support staff that maintain these systems are all minimum qualified and have many years industry experience
- All students use individual logins to allow monitoring of computer usage

DATTA PROTECTION

The school aims to ensure that personal information is dealt with correctly and securely. This applies to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

Data Protection Principles

The school will follow Data Protection Principles as outlined below:

- Personal data is processed fairly and lawfully
- Personal data is obtained only for one or more specified and lawful purpose(s)
- Personal data is adequate, relevant and not excessive
- Personal data is accurate and where necessary, kept up to date
- Personal data processed for any purpose is not be kept for longer than is necessary
- Personal data is kept secure as appropriate to the data
- Personal data is dealt with in accordance to the laws of the UAE

General Guidelines on Data Protection

The school is committed to maintaining the above principles at all times. Therefore the school will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so

- Ensure our staff are aware of and understand our policies and procedures

MONITORING AND REVIEW

The school will monitor Online Safety on an ongoing basis through the logs of use of school Internet and IT Systems along with observations in classes and feedback from students, teachers and parents through surveys and feedback. This policy will be reviewed annually and the findings of the mentioned monitoring will be used to inform improvements and developments of the Online Safety provisions.

SANCTIONS

All members of the school community are expected to comply with the guidelines in this policy. Any violations against the policy will lead to school taking action in accordance with the Student Behaviour Policy or Staff Handbook Guidelines. This may include suspension of access to school internet and IT systems and referral to police or other government agencies if appropriate.

COMMUNICATION OF THIS POLICY

- The policy will be displayed on the school website
- It will be shared via email to all staff, students and parents
- Information sessions will be provided for staff, students and parents through live sessions and pre-recorded videos to ensure all members of the school community are informed of this policy
- The policy will be referenced through the Online Safety Education programmes for students and the wider community on an ongoing basis throughout the year
- It will be shared with students at the beginning of the school year and also shared with any new students as part of their induction
- It will be shared with staff at the beginning of the school year in staff induction and shared with any new staff as part of their induction

Date of Review of this policy: **January 2022**
Date of Next Review of this policy: **January 2023**
Approved by the Management of British International School Ajman

References

UK Council of Internet Safety. (2020). "Education for a Connected World – 2020 Edition" Education for a Connected World - GOV.UK (www.gov.uk)