BRITISH INTERNATIONAL SCHOOL
Dare to Dream

# Acceptable Use Policy for Staff & Visitors

## AIMS OF THIS POLICY

The aim of this Acceptable Use Policy (AUP) is to ensure that staff 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 staff 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 staff (academic and administrative) and any visitors to the school who 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:

- Acceptable Use for Staff and Visitors
- Unacceptable Use for Staff and Visitors
- Responsibilities of Students and Parents
- Monitoring, Reporting and Sanctions
- Acceptable Use Agreements for Staff and Visitors

This policy links with the following policies and guidelines:

- Acceptable Use Policy for Students
- BIS Online Safety Policy
- BIS Child Protection Policy
- Reporting Unacceptable Use and Cyber Bullying Guidelines
- Staff Handbook
- 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.

## ACCEPTABLE USE GUIDELINES

These guidelines for acceptable use of the internet and School IT Systems apply to both **on school premises** and **remote usage** for the purpose of school activities (eg Distance Learning, teacher preparation, and other school activities conducted remotely)

# Acceptable Use Policy for Staff & Visitors

## RESPONSIBILITIES OF STAFF AND VISITORS

- All staff (teachers, leadership and administration) and visitors to the school are expected to promote and support acceptable use within the school and to model good practice.
- Staff are expected to support students at all times in their use of technology and to provide guidance and direction where needed.
- Staff and visitors are required to immediately report any unacceptable use to the school leadership and any other relevant authorities where necessary in accordance with the school's reporting system

## ACCEPTABLE USE FOR STAFF AND VISITORS

- Use the internet and IT Systems in an acceptable and legal manner at all times
- The visitors will be allowed internet access for a time of one hour with limited bandwith access . The wifi password can be obtained from the receptionist on request.
- Staff should communicate with parents through official e mail ids.
- Educate students about appropriate and safe internet usage through scheduled sessions but also at other opportunities that present during classes. This can include guidelines about interaction and communication with other people on social networking websites and in chat rooms
- Encourage awareness about cyber bullying and give clear guidelines as to the steps that are to be taken and people that can be approached
- Monitor and ensure that there is no misuse of internet
- Take immediate and appropriate action (including escalating the issue to relevant leaders in the school) regarding any unacceptable use of cyber bullying found during or outside of classes or any cases reported
- Raise awareness about the advantages and disadvantages of using Social media like Facebook, Twitter, YouTube, Google etc.
- Use the school-sanctioned online web-based platforms to enhance students' education and learning and to facilitate collaborative study habits in students
- Empower students with 20th century learning tools to enable them to become independent learners and global citizens
- Share, educate and promote good practice to avoid plagiarism
- Share outstanding teaching practises through electronic communication
- Incorporate ICT in all areas of the curriculum to encourage the holistic approach of the students
- Develop presentation skills using ICT for project work and competitions
- Encourage students to keep allocated personal username and password confidential, not sharing them with anyone
- Use all digital devices including the school network in a safe and appropriate manner and monitor and promote the same practice for students

## UNACCEPTABLE USE FOR STAFF AND VISITORS

- Accessing, transmitting, copying, or creating material that violates the school's behaviour policy (such as messages/content that are pornographic, sites that promote hatred, discrimination, racism, or meant to harass others)
- Accessing, transmitting, copying, or creating material that is illegal (such as inappropriate or obscene materials, stolen materials, or illegal copies of copyrighted works)
- Using internet to commit any kind of piracy such as music, film or software
- Using resources to further other acts that are criminal or violate the school's behaviour policy
- Using emails, social media, texts or other online platforms to threaten or harass others
- Distributing any information which is incorrect, offensive or slanderous

- Using threatening and inappropriate language in communications
- Instigating or being involved in cyber bullying
- Not reporting cyber bulling when you are aware of it
- Connecting with students on any social media platforms
- Sharing School's confidential matters or information without authorization
- Using the internet to promote personal business including tutoring and other student target activities
- Sending or posting disturbing images on any online platform
- Sharing passwords or using and distributing passwords of others
- Compromising the security of the school's systems by introducing malicious software
- Visiting unauthorised websites
- Damaging or interfering with computers, computer systems, software, or networks
- Deliberately causing harm to someone's work or program
- Changing another person's username, password, files or data
- Using someone else's information or work without permission (plagiarism)
- Disclosing personal information about yourself without authorisation
- Visiting social websites without authorisation

**SCHOOL MONITORING**

- The school is responsible for all internet data that are produced, received or transmitted on the school network. These data can be accessed for requirements such as legal or investigative matters
- All electronic items, both hardware and software, expertise and services involved in the usage of internet belong to the school and the school has the right to access and monitor all data and internet activity which takes place on its systems
- All emails sent through the school email system may be monitored for the safety of all users
- All sites and downloads are monitored and may be blocked if the school considers them unsuitable or inappropriate, or if they are thought to be damaging to the school, staff and / or students
- Unauthorised installation of software is not permitted
- Usage of storage media which is not scanned prior to usage is strictly prohibited in order to limit spread of viruses and other malicious software
- The school reserves the right to take appropriate action, including informing relevant authorities for any unacceptable use of the school's Internet or IT Systems

**MONITORING REVIEW**

The school will monitor the use of the Internet and IT Systems regularly. Monthly monitoring reports will be provided to the Principal and the Online Safety Leader who will review the usage with the Online Safety Group. Any concerns, problems or patterns that emerge from these reviews will be logged. Any actions required will be identified and executed and monitoring will continue to ensure no further issues arise.

**REPORTING**

All members of the school community are required to report any Unacceptable Use of technology within the school or on the school Internet or IT Systems. Further information on how to report an incident can be found by accessing the **"Reporting Unacceptable Use and Cyber Bullying"** guidelines document.

Any staff member must report any Unacceptable Use or Cyber Bullying to the relevant member of staff after taking any appropriate action. This includes the Online Safety Leader, any member of the online safety group, Head of Department, School Counsellor, Section Head, Vice Principal or Principal.

## SANCTIONS

Any violations by staff or visitors of the expectations of this policy including Unacceptable Use and Cyber Bullying will be dealt with in accordance with the school's **Staff Handbook** which is in line with the UAE Labour Law

Sanctions may include, but are not limited to:

- Written warnings
- Conduct hearings
- Dismissal from duty
- Referral to the relevant government authorities where necessary
- Removal of visitors from the school who violate this policy

## REVIEW OF THIS POLICY

The school will review the effectiveness of this policy annually. The monitoring process outlined above will be reviewed, along with logs of incidents and feedback through surveys taken from various groups within the school community.

## COMMUNICATION OF THIS POLICY

- Emailed to staff and included in induction materials at the beginning of the year and new staff
- Given to any visitors who are granted access to the school's internet or IT Systems and will be asked to sign the Acceptable Use Agreement
- Ongoing training throughout the school year for staff to keep them informed of the policy
- Acceptable Use Agreement signed by staff and stored in Staff Files

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

# Staff Acceptable Use Agreement

This agreement must be signed after the staff member has read and understood the Acceptable Use Policy for Staff and Visitors and before being granted access to the school's Internet and IT Systems.

By signing below, I acknowledge that I have read and understand the British International School Ajman's Acceptable Use Policy for Staff and Visitors. I also agree to the following:

- I understand that the school's IT Systems provide me with access to a range of essential learning tools including the internet. I understand that the internet can be a useful teaching resource when used appropriately and agree to do so at all times
- While I have access to the school's Internet and IT Systems, I will only use them for educational purposes to support effective teaching and learning and for school purposes only
- I will not engage in or search for anything that is illegal, inappropriate, dangerous or offensive while using school systems
- I will not reveal my passwords to others, allow anyone else to use my school account or provide access to any school systems, nor disclose personal or school information to others
- I agree to support students at all times in their use of the school's Internet and IT Systems and will provide guidance and instruction in accordance with the Acceptable Use and other School Policies
- I will promote and model good practice at all times in relation to Acceptable Use and will expect students to do the same
- I agree to report any unacceptable use I am aware of including any incidents of cyber bullying
- I understand that, should I choose to use the school's systems inappropriately, action will be taken against me which can include referral to the relevant government authorities and the application of the school's disciplinary procedures

Staff Member's Name: _______________________________________________

Signature: _________________________________________________________

Date: _____________________________________________________________

Principal's Signature: _______________________________________________

# Visitors’ Acceptable Use Agreement

This agreement must be signed after the visitor has read and understood the Acceptable Use Policy for Staff and Visitors and before being granted access to the school’s Internet and IT Systems.

By signing below, I acknowledge that I have read and understand the British International School Ajman’s Acceptable Use Policy for Staff and Visitors. I also agree to the following:

- I understand that the school’s Internet and IT Systems are provided primarily for use of students and teachers for the purpose of enhancing teaching and learning. Being granted access is a curtesy extended by the school which I agree to respect and value
- While I have access to the school’s Internet and IT Systems, I will only use them for acceptable uses as outlined in the Acceptable Use Policy
- I will not engage in or search for anything that is illegal, inappropriate, dangerous or offensive while using school systems
- I will not reveal the password issued to me to others or allow anyone else to use it
- I agree to support students at all times in their use of the school’s Internet and IT Systems and will provide guidance and instruction in accordance with the Acceptable Use and other School Policies should the opportunity arise
- I will promote and model good practice at all times in relation to Acceptable Use
- I agree to report any unacceptable use I am aware of including any incidents of cyber bullying
- I understand that, should I choose to use the school’s systems inappropriately, action will be taken against me which can include referral to the relevant government authorities. I may also be asked to leave the school and may not be granted access to any school systems in the future

Visitor’s Name: ____________________________________________________

Signature: _________________________________________________________

Date: _____________________________________________________________

Principal’s Signature: ______________________________________________