THE BRITISH SCHOOL OF MILAN
LEARNING TO EXCEL SINCE 1969

ACCEPTABLE USE POLICY

1. What is an Acceptable Use Policy (AUP)?

This Acceptable Use Policy sets out the roles, responsibilities and procedures for the acceptable, safe, and responsible use of all digital and communication technologies (including the use of school-based devices, the internet, email, instant messaging, and other social networking technologies, mobile phones, and games) to safeguard adults and students at the British School of Milan. It details how the school will provide support and guidance to parents and the wider community (where appropriate) for the safe and responsible use of these technologies. It also explains procedures for any unacceptable or misuse of these technologies by adults or students.

Associated policies and protocols: E-safety Policy, Staff Code of Conduct, Safeguarding Policy, Behaviour Policy, Anti-bullying and Anti-cyberbullying PolicyAcademic Honesty Policy, Data Protection Policy, Mobile Phone Protocol.

2. Why have an AUP?

The use of the internet as a tool to develop teaching, learning and administration has become an integral part of school and home life. There are always going to be risks using any form of communication which lies within the public domain. Therefore, it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst students use these technologies. These risks include:

- issues with spam and other inappropriate email
- viruses
- grooming by predators
- cyber-bullying
- illegal activities of downloading or copying any copyright materials and file-sharing via the internet or mobile devices
- online content which is abusive, offensive, or pornographic

It is also important that staff are clear about the procedures relating to the AUP (see Staff Code of Conduct); for example only contacting students about homework via a school email address, not a personal one.

Whilst the BSM will endeavour to safeguard and mitigate against all risks, it will never be able to completely eliminate them. Any incidents that may come to its notice will be dealt with quickly and according to policy to ensure it continues to protect students.

It is the duty of the school to ensure that students, teachers, administrative staff, and visitors are protected from potential harm whilst they are on school premises.

The involvement of students and parents is also vital to the successful use of online technologies. This policy thus also aims to explain how parents and students are part of the procedures, and how students are educated to be safe and responsible users so that they can make good judgments about information they see, find, share and use.

ACCEPTABLE USE POLICY

3. Aims of this policy

- to ensure the safeguarding of all students within the school by detailing appropriate and acceptable use of all online technologies
- to outline the roles and responsibilities of all stakeholders
- to ensure all stakeholders are clear about procedures for misuse of any online technologies
- to develop links with parents and the wider community to ensure continued awareness of online technologies.

4. Roles and Responsibilities of the School

4.1 Board of Governors, Principal and Chief Financial Officer

It is the overall responsibility of the Principal and CFO with the Board to ensure that there is an overview of e-safety (as part of the wider remit of Safeguarding) across the school, with further responsibilities as follows:

1. The Principal and teachers are responsible for promoting e-safety across the curriculum.
2. The Principal will inform the Board about the progress of, or any updates to, the e-safety curriculum (via PSHE or ICT) related to safeguarding.
3. The Board must ensure that the DSLs and e-safety Co-ordinator promote a thorough awareness of e-safety and that the e-safety policy illustrates how it is being addressed within the school. It is ultimately the responsibility of the Board to ensure that all Safeguarding guidance and practices are applied.
4. The Principal will ensure the school has an AUP which defines the roles, responsibilities, and safety for using ICT. The Principal and CFO will ensure that any misuse or incident is dealt with appropriately, according to school policy and procedures, and that necessary action is taken even to the extent, if required, of suspending a member of staff, or a student, or involving parents or informing the police.

4.2 Leadership team

4.2.1 Policy and Implementation Management

It is the role of the SLT, together with the ICT Manager, the Director of Academic ICT and the PS ICT Co-ordinator, to ensure appropriate systems and technologies are in place to monitor and maintain the safeguarding and security of all stakeholders using the school network, including:

1. Checking network and perimeter security - CFO
2. Ensuring web filtering is set to the correct level for staff and students in the configuration of the network, stand-alone PCs, school laptops and other mobile devices, and that System Administrators are informed how to adjust it - DAI
3. Using a reputable ISP (Internet Service Provider) - CFO
4. Developing awareness of wireless technology issues - DAI
5. Monitoring of the internet and online technologies - DAI
6. Ensuring that technical staff install appropriate and up-to-date anti-virus anti-spyware and SPAM filtering on the network, stand-alone workstations, school laptops and other mobile devices, and ensuring that these are reviewed and updated on a regular basis - CFO
7. Ensuring that Systems Administrators check for viruses on laptops, stand-alone workstations, tablets and memory sticks, or other transferable media, to minimise issues of virus transfer

8. The use of auto log-off of 15 minutes and regular password changes, adhering to the Deloitte recommendations

4.2.2 Director of Academic ICT

It is the role of the Director of Academic ICT to:

1. Implement agreed policies, procedures, staff training and curriculum requirements, in conjunction with the e-safety Co-ordinator, for ensuring e-safety is addressed in order to establish a safe ICT learning environment
2. Ensure that the AUP is reviewed regularly, with up-to-date information available for all staff to teach e-safety
3. Use the ICT Strategy Steering Group as a forum to discuss technical issues that relate to e-safety
4. Ensure that all stakeholders are aware of the filtering levels and why they are there to protect students and staff
5. Liaise with the Principal so that policies and procedures are up-to-date to take account of any emerging technologies
6. Update staff training in conjunction with the e-safety Co-ordinator according to new and emerging technologies so that the correct e-safety information can be taught and followed
7. Report to the DSLs and Principal all ICT-related safeguarding issues.
8. Ensure web filtering is set to the correct level for staff and students in the configuration of the network, stand-alone PCs, school laptops and other mobile devices, and that System Administrators are informed on the procedures of how to adjust it
9. Developing awareness of wireless technology issues
10. Meet regularly with the e-safety Co-ordinator to discuss relevant e-safety issues and agree appropriate action plans

4.2.3 E-safety Co-ordinator

It is the responsibility of the e-safety Co-ordinator to:

1. Take the lead responsibility for ensuring e-safety is addressed in order to establish a safe ICT learning environment
2. Develop an e-safe culture under the direction of SLT and to promote the school's e-safety vision to all stakeholders
3. Keep a log of incidents via the MIS which can be analysed to help inform future developments and the identification of safeguarding concerns
4. Meet regularly with the Director of Academic ICT to discuss relevant e-safety issues and agree appropriate action plans
5. Act as a key point of contact on all e-safety issues
6. Conduct e-safety audits on an annual basis in conjunction with the SLT
7. Lead an e-safety team (see below)
8. Raise awareness and understanding of e-safety to all stakeholders, including parents and carers, through information evenings and other media
9. Ensure the Acceptable Use Policy is in place, up-to-date and understood by staff, pupils and parents

10. Ensure that the e-safety policy links with other appropriate school policies e.g. Anti-Bullying, Child Protection, ICT, PSHE, etc.
11. Work with the SENCO and DSLs to create e-safety guidance for vulnerable children and those with additional learning needs where necessary
12. Manage e-safety training for all staff in conjunction with Head of Primary School and Deputy Head (Pastoral) of Senior School and ensure that e-safety is embedded within continuing professional development
13. Ensure staff receive relevant information about emerging issues
14. Coordinate e-safety awareness raising/education for pupils and ensure that e-safety is embedded across the curriculum and learning activities, for example, via assemblies and/or theme days
15. Support e-safety awareness raising/education initiatives for parents
16. Act as a point of contact, support and advice on e-safety issues for staff, pupils and parents
17. Report any e-safety incidents to SLT (particularly child protection or illegal issues), and ensure the agreed e-safety incident procedure is followed, as outlined in the school's e-safety policy, maintaining an e-safety incident log and reporting on issues
18. Keep up-to-date with local and national e-safety awareness campaigns and issues surrounding existing, new and emerging technologies
19. Understand the relevant legislation
20. Work with and receive support and advice from recognised e-safety groups and where necessary, liaising with outside authorities and other agencies as appropriate, e.g. the Police
21. Review and update e-safety policies and procedures on a regular basis and at least annually.
22. Set up and lead the E-safety Team: The E-safety Team should include members from all stakeholder groups. The team will help develop and implement policy and practice. It is essential to involve certain members of staff such as DSLs, SENCos and pastoral care staff. This ensures consideration of safeguarding issues from the widest possible perspective.

4.3 Staff and other adults

It is the responsibility of all adults within the school to:

1. Be up-to-date with e-safety knowledge appropriate for the age group with which they work
2. Ensure that they know who the DSL is within school so that any misuse or incidents which involve a student can be reported. Where an allegation is made against a member of staff it should be reported immediately to the DSL and the Principal. In the event of an allegation made against the Principal, the Chair of the Board must be informed without first notifying the Principal.
3. Be familiar with the Behaviour, Anti-bullying, Staff Code of Conduct, Child Protection & Safeguarding, and other relevant policies so that in the event of misuse or a complaint, the correct procedures can be followed. In the event that a procedure is unknown, a staff member must refer to the Principal or a member of SLT immediately
4. Forward requests to unblock videos eg on YouTube that have been denied access by YouTube restricted access to a member of SLT (who will make the decision whether to unblock or not)
5. Alert the Director of ICT and e-safety Co-ordinator to any new or arising issues and risks that may need to be included within policies and procedures or any e-safety incidents in order that they can be centrally recorded via the MIS
6. Ensure that students are protected and supported in their use of online technologies, and that they know how to use them in a safe and responsible manner.

7. Ensure that any students included in images used for promotional purposes eg in the newsletter, on Facebook, Twitter, etc. are not on the list of those who may not be used (as families have not given permission)
8. Use ICT equipment safely and correctly and be responsible for the management of the equipment within their teaching space
9. Not divulge their private email addresses to students or parents, or correspond with them using their private email account
10. Not connect with any current or past BSM student under the age of nineteen on any social networking site
11. Protect confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they are logged on
12. Make sure that any information subject to Data Protection is not stored on portable media or transported in an insecure form
13. Report accidental access to inappropriate materials to the Director of Academic ICT so that the site(s) is/are added to the restricted list
14. Inform a Systems Administrator if they believe there is any security issue with the equipment they are using
15. Use their discretion when communicating electronically about work-related issues and not bring the school's reputation into disrepute
16. Report incidents of personally directed "bullying" or other inappropriate behaviour via the internet or other technologies
17. The school may use Data Loss Prevention software (DLP) to track confidential documents.
18. Use electronic communication in an appropriate way

4.4 Students

Students are:

1. Involved in the review of our Acceptable Use Agreement through the e-safety Committee, in line with this policy being reviewed and updated
2. Responsible for following the Acceptable Use Agreement whilst within school as agreed each academic year or whenever a new student starts at the school for the first time
3. Taught to use the internet in a safe and responsible manner through, for example, ICT and PSHE
4. Taught to tell immediately an adult about any inappropriate materials or contact from someone they do not know.

5. Appropriate use by adults

Staff members, both academic and administrative, have access to the network so that they can access appropriate resources for their classes and work.

All staff receive a copy of the Acceptable Use Policy, which then needs to be signed and returned to school, to be kept on file. The Acceptable Use Policy is available on the School's Network.

Staff are reminded of the need to remain within the remit of the Data Protection Policy, particularly with reference to privacy regarding medical/gender details of pupils.

5.1 In the event of inappropriate use

If a member of staff is believed to have misused the internet or network in an abusive or illegal manner from school, a written report must be submitted to the Principal – who will inform the DSLs and Director of ICT so that details can be centrally recorded. Then the Child Protection & Safeguarding Policy must be followed to deal with any misconduct, and all appropriate authorities contacted.

6. Appropriate use by students

The Acceptable Use Agreements (based on age) are outlined in the Appendices, and detail how students are expected to use the internet and other technologies within school. The rules exist for students to understand what is expected of their behaviour and attitude when using the internet, which then enables them to take responsibility for their own actions; for example, knowing what is polite to write in an email to another student or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This includes the deliberate searching for inappropriate materials and the consequences of doing so.

The downloading of materials, for example music files and photographs, needs to be appropriate and 'fit for purpose', based on research for school work, and be copyright free. File-sharing via email, weblogs or any other means on-line should be appropriate and be copyright free.

The Student Council is encouraged to be involved in discussing the acceptable use of online technologies and the sanctions for misusing them.

Students are taught and encouraged to consider the implications for misusing the internet and, for example, posting inappropriate materials to websites.

6.1 In the event of inappropriate use

Should a student be found to misuse the online facilities whilst at school appropriate sanctions will be applied and the DSLs, e-safety Co-ordinator and Director of ICT informed so that details can be centrally recorded.

If a student accidentally accesses inappropriate materials the student will report this to an appropriate member of staff immediately and take appropriate action to hide the screen or close the window.

Deliberate abuse or damage of school equipment will result in parents being billed for the replacement costs of the equipment.

7. The curriculum and tools for learning

7.1 Internet use

We teach our students how to use the internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding, and communicating effectively in order to

further learning, through ICT and/or PSHE lessons. The following concepts, skills and competencies are taught by the end of Year 11:

- digital citizenship
- future work skills
- internet literacy
- making good judgments about websites and emails received
- knowledge of risks such as viruses, and opening mail from a stranger
- access to resources that outline how to be safe and responsible when using any on-line technologies
- knowledge of copyright and plagiarism issues
- file-sharing and downloading illegal content
- uploading information – knowing what is safe to upload, and not to upload personal
- information
- where to go for advice and how to report abuse.

These skills are taught within the curriculum so that students have the security to explore how online technologies can be used effectively, in a safe and responsible manner.

7.2 Email use

The school provides school email addresses for students (Years 7 to 13) to promote safe and efficient communication in the school. Student email accounts are provided by Outlook. Students should only use their school email for school-related business and they must seek permission from a member of staff to send a mail to the year group email addresses.

Parents are encouraged to engage in a dialogue with their children about the appropriate use of email.

7.3 Mobile phones and other technologies

Students in Senior School may use mobile phones in the classroom for academic reasons only and at the teacher's discretion. Use at other times must be sanctioned by a staff member or used in a 'phone zone'. Staff members should not use their personal phones to contact students. It is our policy to ensure that we educate our students to understand the use of a public domain and the consequences of misusing it, including the legal implications and law enforcement. Primary School and Year 7 students do not use mobile phones in lessons.

Students in the Sixth Form and KS4 are required to bring a laptop to school. Students are expected to bring their device to school fully charged and able to last the school day and to ensure that it is locked away when not in use. Students may use their laptops in the classroom or study areas for academic reasons only. Use of the laptop at other times, or in other locations eg the Dining Room, must be sanctioned by a staff member. Students access documents, files, images, etc via the school wifi therefore subject to the same internet filtering system as on school-owned hardware.

7.4 Video and photographs

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone.

It is not appropriate for staff to use their own personal mobiles or other personal equipment to take photographs of students other than within the use of safe 'apps' such as Frog Snap whereby photos taken are only stored within the app itself and disappear once the app is closed.

Any photographs or video clips uploaded and stored on the school network should not have the full file name of a student. Any images/videos available beyond the school community should only ever include the student's first name. Group photographs are preferable to individual students and should not be of any compromising positions or in inappropriate clothing.

Essentially all images and data relating to students should be secured in the cloud. Staff must delete caches of work documents at home where this relates to student security and safety – this refers also to automatic backups in place on personal devices. Working in the cloud as far as possible should help to minimise risk. Staff must be aware of the published list of students who have requested not to be photographed. This list is updated and shared with all staff by the SS and PS secretaries when any changes are made.

8. Filtering and safeguarding measures

The school's internet has a robust filtering system which is set at an appropriate level such that inappropriate content is filtered. The system logs all attempts to access inappropriate content.

Anti-virus, anti-spyware, Junk mail and SPAM filtering is used on the school's network, stand-alone PCs, laptops and tablets, and is updated on a frequent basis. Security measures are in place to ensure information about our students cannot be accessed by unauthorised users. Strong encryption is used on the wireless network to provide good security.

9. Monitoring

The Director of Academic ICT (with the support of the ICT technicians) is able to monitor the use of online technologies and the use of the internet by students and staff. Incidents of concern will be shared with the Principal and DSLs as appropriate, so that details can be centrally recorded.

10. Computers

The computers in the school are protected in line with the school network policies and procedures. Where software requiring a student login is used, it is password protected so that the student is only able to access him/herself as a user. Students are taught not to divulge their own passwords and to change their passwords regularly.

11. Parents

11.1 Roles

Each student has access to a copy of the school's Acceptable Use Policy. Parents are asked to explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted.

11.2 Support

As part of the approach to developing e-safety awareness with students, the school may offer parents the opportunity to find out more about how they can support the school to keep their child safe whilst using online technologies beyond school. The school wishes to promote a positive attitude to using the internet and therefore asks parents to support their child's learning and understanding of how to use online technologies safely and responsibly. Parents should be aware that the school cannot take responsibility for a student's misuse or abuse of IT equipment when they are not on the school premises. This includes social networking with other students.

12. Links to other policies

12.1 Anti-bullying and Anti-Cyberbullying Policy

Please refer to the Anti-bullying and Anti-Cyberbullying Policy for school procedures when managing allegations of bullying and incidents via any online communication, such as mobile phones, email or blogs.

12.2 Managing Allegations Against Staff and the Safeguarding Policies

Any incidents involving the alleged misuse or abuse of personal mobile or email technologies should be reported to the Principal immediately, or the Chairman of the Board in the event of the allegation being made about a Principal.

No personal email address or phone numbers should be used when contacting students about homework or any other school issues either in or beyond school. We follow this procedure to protect staff members from potential allegations of misconduct by a student or parent.

Please refer to the Child Protection and Safeguarding Policy for the correct procedure in the event of a breach of child safety, and inform the DSL immediately.

12.3 School websites

The uploading of images to the school websites is subject to the same rules as uploading to any personal online space.

12.4 Disciplinary procedure for staff to follow

In the event of a student being in breach of behaviour and good conduct through misuse of online technologies, the following procedure should be followed by staff:

ACCEPTABLE USE POLICY

1. An inappropriate website is accessed inadvertently
Inform the Principal and Director of Academic ICT in writing so that details can be centrally recorded. Contact the helpdesk via email so that it can be added to the banned or restricted list.
2. An inappropriate website is accessed deliberately
Ensure that no one else can access the material, by shutting down the computer. Inform the Director of Academic ICT in writing so that details can be centrally recorded. Report to the Principal referring to the Acceptable Use rules and follow agreed actions for discipline.
3. An adult receives inappropriate material
Do not forward this material to anyone else – doing so could be an illegal activity. Ensure the device is shut down, and inform the Director of Academic ICT in writing so that details can be centrally recorded.
4. An adult has used ICT equipment inappropriately
Follow the procedures for 2.
5. An adult has communicated with a student, or used ICT equipment, inappropriately

- Ensure the student is reassured.
- Report to the Principal, DSL and e-safety Co-ordinator, who should then follow the Safeguarding Policy including recording the details of the incident.
- Preserve the information received by the student if possible, and determine whether the information received is abusive, threatening or innocent.
- If illegal or inappropriate use is established, contact the Principal (if allegation is made against the Principal, then contact the Chairman of the Board) and the DSL for safeguarding immediately, and follow the Safeguarding Policy.

6. Threatening or malicious comments are posted to the school website or distributed via the school email system (or printed out) about an adult in school:

- Preserve any evidence
- Inform the Principal immediately

7. In cases where a student, parent or staff member considers that images of staff or adults have been posted on inappropriate websites, or have inappropriate information about them posted anywhere, the Principal must be informed.

GDPR – overview of key considerations linked to the AUP

Do

- Change password and make complex
- Check content of email
- Ensure you are sending to the right person
- Delete if you no longer need data (max 10 years)
- Keep data securely and store remotely
- Always log-off (auto-lock)

Don't

- Forward personal data to third parties eg exam results
- Use pendrives
- Keep sensitive info on personal devices
- Retain info unless legitimate interest

ACCEPTABLE USE POLICY

Acceptable Use Rules/Agreements according to age group

Reception and Key Stage 1
These are our rules for using the internet safely at school.

- We use the internet safely to help us learn
- We learn how to use the internet
- If we see anything on the internet, or receive a message, that is unpleasant, we must inform an adult
- We can write polite and friendly emails or messages to people whom we know
- We only use our first names when communicating electronically
- We learn to keep our password a secret
- We know who and when to ask for help
- If we see something on a computer that we do not like we know what to do
- We know that it is important to follow the rules
- We aim to look after each other by using the internet safely.

Key Stage 2 (Years 3-6)
These are our rules for using the internet safely and responsibly at school.

- We use the internet to help us learn, and we will learn how to use the internet safely and responsibly
- We send emails and messages that are polite
- Approval from an adult may be needed before we email, chat to, or video-conference anyone at school
- We never give out passwords or personal information (like our last name, address or phone number)
- We never post photographs or video clips without a teacher's permission and never include names with photographs
- We never take images without permission or use images to cause upset or to bully
- If we need help we know who and when to ask
- If we see anything on the internet or in an email or other electronic message that makes us uncomfortable or appears unpleasant, we inform an adult
- If we receive a message sent by someone we do not know, we inform an adult
- We aim to look after each other by using our safe internet in a responsible way

ACCEPTABLE USE POLICY

Senior School (Year 7-13)

Acceptable Use Agreement

- I will only use ICT systems in school, including the internet, email, digital video and mobile technologies for school purposes
- I will check my school emails at least once every working day (twice a day if in the Sixth Form)
- I will only use my school email address for any communication with teachers or other students on a work related issue
- If I wish to use my school email address for communication on school related business e.g. university applications, then I will ask permission from a member of staff and copy that member of staff into the email
- I accept that the school may monitor my use of the internet at school and my school email account
- I will report any problems accessing email or the cloud immediately to the Director of Academic ICT
- I will not download or install software on school technologies
- I will only log on to the school network, other systems and resources with my own username and password and I will keep my username and password confidential and change my password regularly
- I will not browse, upload, download or forward material that could be considered offensive or illegal. I accept that breaching this will lead to disciplinary action and my parents may be contacted. If I accidently come across any such material I will report it to my teacher immediately
- I will not respond to offensive, abusive or rude messages. I will let a teacher know immediately if I am sent anything I do not feel comfortable with
- I will not give out or make available any personal information such as my full name, phone number or address to someone unknown to me. I will not arrange to meet someone offline that I have met only online unless it is part of a school project and approved by a teacher/parent
- I am aware that when I take images of pupils and/or staff I must only store and use these for school purposes in line with school policy and must never distribute these outside the school network without the permission of all parties involved. This agreement extends to school break times, school trips and all occasions when I am in school uniform or otherwise representing the school
- I will support the school approach to e-safety and ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring the school community into disrepute. This includes
    - What I write on a computer – I will check my work before I print or sent it
    - Not using bad language – I will not write racist, sexist, abusive, homophobic or aggressive words
- I will not access, create or display any material (images, sounds, text, and video) which is likely to cause offence, inconvenience or anxiety to anyone
- I will think before I print to minimise the amount of paper I use
- I will not attempt to bypass the internet filtering system
- I do not assume that information published on the web is accurate
- I will respect the privacy and ownership of others' work online at all times
- I will not copy images from the internet and pass them off as my own

ACCEPTABLE USE POLICY

- If I quote from a text I will always attribute my sources and acknowledge use of anyone else's ideas, images or data by citing the author and compiling a bibliography
- I will follow the school and IB rules on academic honesty and not practise plagiarism
- I will report to a teacher any incident that breaches the Acceptable Use Agreement, even if that incident does not affect me
- I treat school ICT equipment with respect and will report any damages to a teacher
- If I deliberately damage a piece of school equipment I will be charged for its replacement

Student agreement:

Name: _____Grade:_____

I understand the rules for using the internet, email and online tools safely and responsibly. I am aware that the adults working with me at school will help me to check that I am using technology appropriately.

Student signature: _____ Date: _____