

# Acceptable Use Policy

AUP Policy



2020

# Acceptable Use Policy

**BOSTON NS**

- 1. Introduction**
- 2. School's Strategy**
- 3. Use of the Internet**
- 4. Email / Google Drive**
- 5. Distance Learning**
- 6. Internet Chat**
- 7. School Website and affiliated Social Media sites.**
- 8. Personal Devices**
- 9. Legislation and Regulation**
- 10. Support structures and Education**
- 11. Use of Information Communication Technology ("ICT") Resources**
- 12. Sanctions**
- 13. Policy Approval/Ratification**

## **APPENDIX – Permission Slip**

## 1. Introduction

The aim of the Acceptable Use Policy (“AUP” or “the Policy”) is to ensure that students benefit from the learning opportunities offered by internet access in a safe and positive manner. This Policy also aims to establish minimum standards for, and let the students, parents/guardians know of the school’s administration and monitoring of, the schools devices, equipment and networks.

This Policy applies to all of the school’s “Devices”, which means all computers, iPads, laptops, smart phones and other IT resources that connect to the school’s network.

This Policy applies to staff and students of Boston National School (“the School”). The School reserves the right to amend this policy from time to time entirely at its discretion.

This Policy should be read carefully to ensure that the content is accepted and understood. This AUP was updated by the school in September 2020.

## 2. School’s Strategy

The School employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet.

These strategies include, but are not limited to the following:

- Internet sessions which are conducted on school Devices will always be supervised.
- Websites will be previewed / evaluated by a teacher using a filtering system, before being integrated into lessons conducted on school Devices. The School’s search engine has a built in ‘safe search’ feature. The ‘safe search’ feature will be enabled on all search engines on school Devices.
- A firewall is used on school Devices to minimise the risk of exposure to inappropriate material and to block unsuitable sites. This is regularly updated.
- Students will be provided with training by teachers in the area of research techniques specific to the Internet.
- Teachers will take part Continuing Professional Development (CPD)
- Online safety training will be provided to teachers and will be taught to all students.
- Uploading and downloading of non-approved software on school Devices will not be permitted.
- Virus protection software is used on school Devices and updated regularly.
- The use of encrypted/password protected Personal External Storage Devices in school is permitted, while email / cloud storage is preferred.
- It is important to note that the school’s Anti-Bullying Policy should be read in conjunction with this Policy. Parents/guardians and students should be aware that placing a once-off, offensive or hurtful internet message, image or statement on a social network site or other public forum where that message, image or statement can be viewed and/or repeated by other people will be regarded as bullying behaviour.

### 3. Use of the Internet

- Students will be taught specific lessons on online safety by teachers.
- Students will not knowingly attempt to visit Internet sites on school Devices that contain obscene, illegal, hateful or otherwise objectionable materials and the school will not be responsible for any attempts taken in this regard. Students who do so will be subject to the sanctions detailed below.
- In the event of accidentally accessing any of the above sites, the student will be expected to immediately turn off the monitor and report the incident to a teacher or supervisor.
- The internet will be used to enhance learning and will be used for educational purposes. All websites used by the teacher will be vetted in advance by the teacher.
- Students will not upload, download or otherwise transmit material that is copyrighted on school Devices.
- Students will not disclose or publicise personal or confidential information to others online. Examples of this are, but not limited to, their own or classmates' home addresses, telephone numbers, email addresses, online profile information or name and location of their school.
- Students will not examine, change or use another person's files, username or passwords.
- Students will be aware that any usage, including distributing or receiving any information, school-related or personal, may be monitored for unusual activity, security, and/or network management reasons.
- The school takes every reasonable precaution to provide for online safety, but it cannot be held responsible if students access unsuitable websites either deliberately or inadvertently.

### 4. Email

- Students will not send or receive any material that is illegal, obscene, defamatory, or that is intended to annoy or intimidate another person.
- Students will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.
- Students will never arrange a face-to-face meeting with someone they only know through emails or the Internet.
- Students will note that sending and receiving email attachments is subject to permission from their teacher.

### 5. Distance Learning

- In circumstances where teaching cannot be conducted on the school premises, teachers may use Zoom, SeeSaw, Padlet or other such platforms approved by the Principal as platforms (the "Online Platforms") to assist with remote teaching where necessary.
- The school has signed up to the terms of service of the Online Platforms in use by the school.
- The School has enabled the most up to date security and privacy features which these Online Platforms provide.
- Parents/guardians will be provided with the password and will monitor their child's use of the Online Platforms.

- If teachers are using Zoom, parents/guardians will consent to their child having access to the lessons. Parents may consent by submitting their own email address for their child to access lessons on Zoom.
- Parents/guardians must monitor their child's participation in any such lessons conducted on the Online Platforms.

## 6. Internet Chat

- Discussion forums on Seesaw or Zoom will only be used for educational purposes and will be supervised.
- Students will never arrange a face-to-face meeting with someone they only know through emails or the Internet and this is forbidden

## 7. School Website and affiliated Social Media sites.

- The school's website address is: [www.bostonns.com](http://www.bostonns.com)
- The School's Facebook account is "Boston National School"
- Students will be given the opportunity to have photos, projects, artwork and other work relating to curricular and extra-curricular school activities published on the school website and media platforms as per the consent form. Teachers will coordinate the publication of this material.
- Personal information relating to the student including their name, home address and contact details will not be included on school social media or the school's website.
- Digital photographs and audio or video clips of individual students will not be published on the school website and/or affiliated pages, without prior parental/guardian permission. Instead, photographs etc. will focus on group activities, where children will not be named.
- Photos/Videos may be used for the production of the Homework Journal or specific school events e.g. Communion etc. These photos/videos and the photos/videos on our website/Facebook page should not be copied or posted to any social media or other website or published in any way.
- Parent(s)/guardian(s) are requested **not** to 'tag' photographs or any other content which would identify any children or staff in the school. Photos should **not** be tagged including geo tagging as this will provide information not in line with GDPR guidelines.
- Parent(s)/guardian(s) are requested to ensure that online messages and/or comments to the school's social media sites are respectful. Any messages written on social media are treated in the same way as written messages to the school.
- The Principal will review the content of the website and the social media sites regularly. The Principal and the Board welcome any suggestions about how the content may be improved.
- If any parent or guardian has any concern about the appropriateness of the content of the website or social media sites, then the Board asks that the matter be brought to the attention of the Principal as a matter of urgency.
- This Policy should be read in conjunction with our Data Protection Policy.

## 8. Personal Devices

- Students may not use any personal device with recording or image taking capability while in school or on a school outing. Any such breach of the Acceptable Use Policy (AUP) will be sanctioned accordingly.
- Any images or recordings taken by class teachers on smartphones or other personal devices must be downloaded onto the school server and/or on to the relevant school affiliated website and then immediately deleted from source.
- The use of E-readers may be permitted, under the supervision of the teacher. All personal devices are to be turned off during school hours.

## 9. Legislation and Regulation

The school will provide information on the following legislation relating to use of the Internet with which teachers, students and parents/guardians should familiarise themselves where appropriate:

- EU General Data Protection Regulations 2018
- Anti-Bullying Guidelines for Primary Schools 2013
- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1998
- Video Recording Act 1989
- The Data Protection Act 1988
- Interception Act 1963

## 10. Support structures and Education

- The school will inform students and parents/guardians of key support structures and organisations that deal with illegal material or harmful use of the Internet.
- The school will run a programme on acceptable internet usage for students. This will cover several topics including cyber-bullying. Parents/guardians will also be provided with information of appropriate courses, talks and literature on the subject.
- Staff will regularly partake in Continuous Professional Development in relation to the development of AUPs, internet safety and cyber-bullying.

## 11. Use of Information Communication Technology (“ICT”) Resources

- Boston National School’s information and technology resources (e.g. e-mail, computers, computer applications, networks, internet, intranet, facsimile, phone and other wireless communications devices, telephone, paging and voice mail systems and the like) are school property and are provided solely for school related activities.
- Inappropriate use including hacking, pirating software, using school resources for non-school commercial activities, soliciting, distributing literature for outside entities, disclosing confidential information of the school, sending inappropriate e-mail or accessing inappropriate web sites (such as those advocating hate or violence, containing sexually explicit material promoting illegal

activities), or using school resources in a way that violates the letter or spirit of the school's policies or reflects negatively on the school is forbidden.

- Users of the school's information and technology resources must not share passwords. If you allow others to use your password or assigned resource, you will be held responsible for their use.
- Consistent with national laws, the Board of Management reserves the right to monitor the use of its information and technology resources and to take appropriate disciplinary actions, or denying future access privileges in cases of misuse. Staff/student use of the school's information and technology resources constitutes consent to such monitoring. All such monitoring will be conducted in accordance with law including, where applicable, the EU's General Data Protection Regulation ("GDPR").

## **12. Sanctions**

- Misuse of the Internet or any activity which is in contravention with this Policy, may result in disciplinary action, including written warnings, withdrawal of access privileges, and, where appropriate, suspension or expulsion in line with the Code of Behaviour.
- The school also reserves the right to report any illegal activities to the appropriate authorities.
- Access to the Internet will be withdrawn from students who fail to maintain acceptable standards of use.

## **13. Policy Approval/Ratification**

The policy was ratified by the Board of Management of Boston NS at its meeting held on \_\_\_\_\_.

Signed: \_\_\_\_\_ Chairperson, Board of Management

APPENDIX 1

Dear Parent(s)/Guardian(s),

The staff and Board of Management of Boston National School have recently reviewed the school's Acceptable Use Policy (A.U.P). Please familiarise yourself with this policy, prior to completing the A.U.P Permission Slip. School files will be updated accordingly and this form will be kept on file for no longer than is necessary.

**Acceptable Use Policy Permission Slip**

Name of student: \_\_\_\_\_ Class/Year: \_\_\_\_\_

Parent/Guardian,

As the parent or legal guardian of the above student, I have read the Acceptable Use Policy and grant permission for my child to access the Internet. I understand that students may not be able to participate fully in lessons involving PCs, laptops, iPads, tablets and other IT equipment without consenting to our Acceptable Use Policy.

Parent/Guardian Signature: \_\_\_\_\_ Date: \_\_\_\_\_

**Inclusion of photos on School Website and Media Platforms**

I understand that, if the school considers it appropriate, my child's schoolwork and group images of activities may be chosen for inclusion on the school website or Facebook page. I understand and accept the terms of the Acceptable Usage Policy in relation to publishing pupils' work and photographs of school activities on the website.

Parent/Guardian Signature: \_\_\_\_\_ Date: \_\_\_\_\_