BRYANSTON PARALLEL MEDIUM
SLOANESTRAAT/STREET POSBUS / P O BOX 69188 BRYANSTON
2021

Hoof: R. Kachelhoffer
Tel: 011 463 1414/5/6
Fax: 011 706 7764
E-mail: principal@bpms.co.za

BRYANSTON PARALLEL MEDIUM SCHOOL
ICT ACCEPTABLE USE POLICY

1. INTRODUCTION

1.1 The use of digital technology and the Internet has become an integral part of the medium of education offered by BPMS. BPMS recognises the need for students to be safe and responsible users of digital technologies, both at home and at school. It is therefore essential that students are taught about safe and responsible online behaviour in partnership with BPMS and Parents/Guardians.

1.2 This policy document and the rules and guidelines contained herein, has been prepared in consultation with students, parents, teachers and staff and has been approved by the School Governing Body.

2. PURPOSE

2.1 BPMS owns and operates a variety of computing systems, including, but not limited to, the BPMS Network, which are provided for the use of BPMS students, teachers and staff in support of the programs of the School. BPMS recognises that students own, or are in possession of, their own personal digital devices with access to the Internet including, but not limited to, tablet devices, mobile devices and personal computers.

2.2 Access to the BPMS Information and Computer Technology (ICT) Network is provided for students as a tool for educational use only and access to this resource is a privilege which carries with it responsibilities. Student behaviour concerning the use of e-mail, Internet and network resources must be used according to the principles outlined in this policy. These rules are intended to

facilitate the appropriate, effective and equitable use of the BPMS network for all members of the BPMS community.

2.3 Any computing system and device, whether owned by the School, student or teacher, which are utilised on school premises at any times, are to be used for education, research, academic development, and public service only, and according to the rules and guidelines set out in this document. All users of these systems are responsible for seeing that these computing systems and devices are used in an effective, efficient, ethical, and lawful manner.

2.4 This document establishes rules and prohibitions that define acceptable use of these systems and devices. Unacceptable use is prohibited, and is grounds for loss of ICT privileges, as well as discipline or possible legal sanctions. It is important that all students, parents and teachers understand the expectations contained in this policy and abide by them at all times. The conduct expected when using the BPMS Network must reflect the high standards of behaviour expected from all members of the BPMS community at all times.

3. USE OF BPMS NETWORK AND ONLINE BEHAVIOUR:

3.1 Students will be provided with an individual username and password to access the BPMS network, which must always be kept secure.

3.2 Students must only access the BPMS network using their own username and password.

3.3 Students must not intentionally access, interfere with, copy or move other students' files or settings, whether they are contained on the BPMS network or on any device.

3.4 Students must not intentionally interfere with, move or delete shared files stored on the BPMS network.

3.5 Students must not install or store inappropriate or illegal software on their devices or on the BPMS network or BPMS devices.

3.6 Students may only utilise the BPMS network to host or participate in game playing if this has been approved by a teacher or the principal.

3.7 Students must not utilise the BPMS network, any other network or any social media platform as a medium to bully, harass, threaten, intimidate or defame other users of the BPMS network or any other person or entity. Students are reminded that their behaviour on-line should reflect their behaviour offline or in person. Students must treat others fairly and with common courtesy. Failure to adhere to this rule will result in disciplinary action or sanctions being taken against students, and both parents and students are warned that such conduct could attract criminal and/or civil liability.

3.8 Students who are experiencing harassment or bullying online are advised not to respond thereto and are urged to record all details of the offending conduct and to save any information in this regard. Students must immediately notify a teacher and/or the principal and/or their parents/guardians of the offending conduct.

3.9 Students who, for whatever reason, feel uncomfortable or unsafe whilst being online, must immediately report this to their teacher and/or the principal and/or their parents/guardians.

3.10 Students are reminded that they have a responsibility to report to their teacher, and/or the principal, and/or their parents/guardians of any unsafe, inappropriate or hurtful online behaviour committed by anyone.

3.11 Students are reminded that file sharing between their devices over the BPMS network, or any other network, can be a security risk and students are urged to avoid allowing other students access to their devices.

3.12 Students are reminded and urged to take steps to protect their privacy when utilising the BPMS network and or their devices. Students must not provide their personal information, full names, telephone numbers, e-mail addresses, residential addresses, usernames and passwords, or images of themselves to any person or entity whilst online.

4. INTERNET USAGE

4.1 Internet access provided through the BPMS network is provided for educational use only and not personal use. Students are reminded that all internet use through the BPMS network is logged and may be reviewed at any time, and at the sole discretion of the BPMS ICT Technician or the principal.

4.2 Students may only access the Internet during class time (whether it's through the BPMS network or any other network) with the express permission from their teacher.

4.3 All Internet usage by students during class time will be supervised by their teacher.

4.4 The Internet connection provided through the BPMS network is filtered to prevent access to online content which is deemed inappropriate for School use and no student should attempt to circumvent this security feature.

4.5 Whilst BPMS undertakes to take all reasonable steps to filter inappropriate content through the BPMS network, it acknowledges that full protection from inappropriate content is not guaranteed and all students, teachers and staff have a duty to notify the BPMS ICT Technician and/or the principal in the event that they become aware of any inappropriate content being accessed through the BPMS Network or any other network on the School's premises by anyone.

4.6 Students must exercise care when using the Internet and should not seek to access or download inappropriate, offensive, discriminatory or intimidating content and/or material.

4.7 Accessing, storing or distributing material that is inappropriate, offensive, discriminatory or intimidating in nature, or which puts any member of the BPMS community at risk, is contradictory to the ethos of BPMS and will lead to disciplinary action. To the extent that the accessing of, or storing of, any content or material that contravenes the Laws of the Republic of South Africa, BPMS will be obliged to report such conduct to the appropriate authorities.

4.8 Students must exercise caution when downloading files off the Internet as these may contain viruses, adware or spyware. Anti-virus software is provided as part of the access to the BPMS network and students must scan their devices regularly to ensure that it is free from infections.

4.9 Students must exercise caution when entering their personal details online, such as submitting their e-mail addresses to a website. Students must ensure that all sites that they access on the Internet is secure. If a student is unsure regarding the safety of any website on the internet, they must immediately notify their teacher. Unsolicited e-mails (such as SPAM) may be considered offensive, inappropriate and unsafe and can place the students, their devices and the BPMS network at risk.

4.10 BPMS reserves the right to, at any time, and without prior notice, examine e-mail messages, files stored on students' devices and in network locations, internet favourites, history and cache files, and other information stored on devices and on the network, for material that would constitute a breach of this policy.

4.11 BPMS will not be responsible for any loss or liability incurred by any student, teacher or staff member through the use of the Internet through the BPMS network or any other network.

5. USE OF DEVICES AT SCHOOL

5.1 All students, parents and teachers acknowledge that the use of devices, and in particular tablet devices ("tablets") have become an integral part of the medium of education at BPMS and are intended for use at school each day. In addition to teacher expectations for the use of tablets, school messages, announcements, calendars and schedules will be accessed using the tablet.

5.2 Similar to their textbooks, students are responsible for bringing their tablets to school and their classes each day, unless specifically advised not to do so by a teacher.

5.3 In the event that a student has left their tablet at home, they must take immediate and reasonable steps to contact their parents to bring the tablet to School.

5.4 Students must ensure that their tablets are fully charged before bringing the tablets to School.

5.5 In the event that a student's tablet is not in working order for whatever reason, the school will issue a "loaner tablet" to that student until such time as their tablet has been repaired and/or replaced.

5.6 Students may not use inappropriate media as a screensaver on their tablets whilst on school premises. The presence of, *inter alia*, guns, weapons, pornographic materials, inappropriate language, alcohol, drugs and drug related paraphernalia, gang-related symbols or pictures in screensavers or as background images is strictly forbidden. Failure to adhere to this rule may result in disciplinary action or sanctions being taken.

6. USE OF CAMERAS

6.1 BPMS will educate all students, teachers and staff about the risks of taking, using, sharing, publication and distribution of images online.

6.2 Students must not take, use, share, or publish any images or video of others in the BPMS community without their consent. Failure to adhere to this rule may result in disciplinary action or sanctions being taken.

6.3 Teachers and staff are permitted to take digital/video images to support educational aims, but must follow school policies concerning the distribution of those images or video, which should only be taken on school equipment and stored on the BPMS network.

6.4 When taking pictures or video images, teachers must ensure that students are appropriately dressed and are not participating in activities that might bring individuals or the school in disrepute.

6.5 Pictures or video which is published on the school website, or elsewhere, which include pupils will be selected carefully and will comply with good practice guidance on image use.

6.6 Students' full names will not be used anywhere on a third-party website or blog, particularly in association with photographs.

6.7 Written permission from parents or guardians will be obtained before photographs of students are published on the school website, or any other third party website or blog.

6.8 Student work can only be published with the permission of the student, and/or their parent(s)/guardian(s).

7. USE OF SOCIAL MEDIA AND CHATROOMS AT SCHOOL

7.1 Students are not allowed to access any online social media from any device whilst a class is in session, without the express permission from their teacher or the principal. This includes, but is not limited to, Facebook, Twitter, Instagram, Snapchat, WhatsApp, Tumblr, Vine, etc.

7.2 Students are not allowed to access any online social media through the BPMS network without the express permission of their teacher or the principal.

7.3 Students will not be allowed to access public or unregulated chatrooms through the BPMS network without the express permission of their teacher or the principal.

7.4 Students are reminded of what is stated above regarding their conduct when being online. Under no circumstances must any social media platform (or any other platform) be used to bully, harass, threaten, intimidate or defame any other member of the BPMS community or any other person or entity. Parents and students are reminded again that such conduct could result in disciplinary action or sanction(s), including criminal and/or civil liability.

8. ACCEPTABLE USE OF ICT

8.1 <u>General Guidelines</u>:

8.1.1 Students will have access to all available forms of electronic media and communication which is in support of education and research and in support of the educational goals and objectives of BPMS.

8.1.2 Students are responsible for their ethical and educational use of the technological resources of BPMS.

8.1.3 Access to BPMS technology resources is a privilege and not a right. Each employee, student and or parent/guardian will be required to follow the acceptable use policy.

8.1.4 Transmission of any material that is in violation of any South African law is prohibited. This includes, but is not limited to the following: confidential information, copyrighted material, threatening or obscene material, and computer viruses.

8.1.5 Any attempt to alter data, the configuration of a device or the files of another user, without the consent of the individual, or the BPMS ICT Technician, will be considered an act of vandalism and subject to disciplinary action in accordance with the BPMS Policy Handbook.

8.1.6 In the event that a student loaned his or her device to a fellow student, it remains the responsibility of the owner of the device to ensure that all content adheres to the ICT policy of BPMS

8.2 Privacy and security:

8.2.1 Students must not go into chat rooms or send chain letters without permission;

8.2.2 Students must not open, use, or change computer files that do not belong to them;

8.2.3 Students must not reveal their full name, phone number, home address, credit card number(s), password(s) or password(s) of other people.

8.2.4 Students are reminded that storage is not guaranteed to be private or confidential on the BPMS network.

8.2.5 If a student inadvertently accesses a web site containing obscene, pornographic or otherwise offensive material, the student has a responsibility to notify a teacher or the principal immediately so that such sites can be blocked from further access.

8.3 Legal propriety:

8.3.1 Students must comply with trademark and copyright laws and all license agreements. If a student is unsure, they must ask a teacher, the principal or their parents/guardians.

8.3.2 Students are reminded that plagiarism is illegal and a violation of the BPMS policy handbook. Students must give credit to all sources used in their own work, whether quoted or summarised. This includes all forms of media on the Internet such as graphics, pictures, movies, music and text.

8.3.3 Students are reminded that the use or possession of hacking software is strictly prohibited by the Electronic Communication and Transaction Act 25 of 2002 and violators will either be subjected to criminal prosecution or the consequences listed in the BPMS policy handbook. Violation of any applicable law of the Republic of South Africa, including the code of the Department of Education, will result in criminal prosecution or disciplinary action.

8.4 E-mail:

8.4.1 Students must always use appropriate language when sending e-mails;

8.4.2 Students must not transmit language or material that is profane, obscene, abusive or offensive to others;

8.4.3 Students must not send mass e-mails, chain letters or spam.

8.4.4 Students should maintain high integrity with regard to all e-mail content authored by them;

8.4.5 Students must not engage in private chatting through their devices during class without permission from a teacher or the principal;

8.4.6 Students are reminded that all e-mail sent using the e-mail address provided by BPMS to students, is subject to inspection by the school to ensure appropriate use;

8.4.7 Students must not e-mail games or game installation files to other students or any other person;

8.4.8 Students must take care to monitor the total size of their mailbox and take steps to maintain their data within the allowed storage limits

8.5 Consequences:

8.5.1 The student in whose name a system account is issued, and who is in possession of any device with access to the Internet, will be responsible at all times for its appropriate use. Non-compliance with the policies of the ICT Acceptable Use policy will result in disciplinary action and/or sanctions as outlined in the BPMS policy handbook.

8.5.2 Electronic mail provided by the school, BPMS network usage and all stored files on the BPMS network shall not be considered confidential and may be monitored at any time by designated BPMS staff to ensure appropriate use.

8.5.3 In the event that any student is found to have contravened this ICT policy, a meeting will be called with that student's parent(s)/guardian(s) and the principal in order to discuss the contravention and the appropriate sanction(s). Pending the convening of such a meeting, and depending on the nature and seriousness of a student's breach of the ICT policy, BPMS reserves the right to limit and/or remove a student's access to the BPMS network and/or confiscate a student's device and/or limit or remove a student's access to BPMS computers or devices.

8.5.4 In the event that the school deems it necessary and appropriate to confiscate a student's device, the parents/guardians of that student will immediately be contacted and the device in question will only be released directly to the parents/guardians.

8.5.5 Parents specifically acknowledge that the confiscation of any device is not deemed to be spoliation of private property as the device in question will be handed to parent(s)/guardian(s) immediately once they attend the school's office to collect same.

9. BACKUP

9.1 Student's devices will be set up with a "My Documents" folder in which students should save their work. This folder will automatically save a copy of all student documents saved to the "My Documents" folder on the BPMS server while they are on the BPMS network. When a student adds a document to the "My Documents" folder while working at home or away from school, that document will be copied automatically to the BPMS server when the student logs onto the BPMS network.

9.2 Only files stored in "My Documents" will be automatically backed up and saved. Student work saved to a different location on their device will not be saved to the school server.

9.3 Students must not use their space on the BPMS network to store extremely large files, or personal files such as music, pictures, videos, games, etc. Students must monitor the total size of their network folder and maintain their data within the allowed storage limits.

9.4 BPMS will not be responsible for any data stored outside a student's personal "My Documents" folder.

10. SECURITY AND CARE

10.1 Students must take care to maintain their devices in good working condition. If any problem occurs with a device, students must contact the BPMS ICT Technician so that the issue can be resolved and the device returned to them.

10.2 Parents are urged to insure their children's devices.

10.3 Students must always carry their devices in a protective cover.

10.4 Students must keep their devices locked up, or in their possession. Students must take care to ensure that other students cannot gain access to their locker and they must always keep their combination secure.

10.5 If a student misplaces their device, they should immediately report this to the BPMS ICT Technician and/or a teacher, who will in turn take reasonable steps to locate the device.

10.6 If a student finds a device and the owner cannot immediately be located, the student must promptly hand it to the BPMS ICT Technician or their teacher so that the owner can be found.

11. GENERAL PRECAUTIONS WITH DEVICES

11.1 Students must not bring any food or drink is allowed next to your tablet while it is in use.

11.2 Students should never carry their tablet while the screen is open.

11.3 Student's devices should be logged out and placed in a protective sleeve when moved between classes.

11.4 Some carrying cases can hold other objects (such as folders and workbooks), but these must be kept to a minimum to avoid placing too much pressure and weight on the tablet screen.

11.5 Student's devices must be turned off before placing it in the carrying case for extended periods of time.

11.6 The screens on certain devices can be damaged if subjected to rough treatment, especially from excessive pressure on the screen. Students must not lean on their devices when closed or put anything near or on the device which would place pressure on the screen.

11.7 Student's tablets must never be left in a car or any unsupervised area.

11.8 Students are responsible for keeping their tablet's battery charged for school each day.

11.9 Student's devices must be labelled in the manner specified by the school. Devices can be identified by their serial numbers and students and parents are urged to keep a record of the serial numbers of their children's devices.

12. HOME NETWORKS

12.1 BPMS recognises that a student's device may be connected to a network outside the school, however it is important that students understand that certain work undertaken by the BPMS ICT Technician in order to ensure that devices function as required at school, can affect, and in some cases, erase these settings.

12.2 Students and parents are responsible for recording student's home network settings and passwords – Students and/or parents should ask the person who set up their home network to provide these to you. Any support provided by the BPMS ICT Technician for non-BPMS networks is provided on a best-effort basis only, and should not be an expectation of the service provided by the BPMS ICT Technician.

13. SOFTWARE ON YOUR TABLET

13.1 The software originally installed by BPMS must remain on student's devices in usable condition and be easily accessible at all times.

13.2 Student's devices will be provided with anti-virus protection software. The anti-virus software will be upgraded from the BPMS network. The School's storage server and e-mail server are also installed with anti-virus protection software and hardware.

13.3 It is the responsibility of individual students to be aware of additional software programs and files loaded onto their devices. Students are responsible for maintaining the integrity of software required for facilitating academic activities.

13.4 Any additional software on student's devices must be appropriate for the school environment and may not infringe on the productivity of the classroom setting.

13.5 Students are responsible for ensuring that only software that is licensed to their device is loaded onto their devices.

13.6 Violent games and computer images containing obscene or pornographic material are prohibited from student's devices whilst on school premises.

13.7 If technical difficulties occur or illegal software is discovered, the ICT Technician will copy all files in the My Documents folder. The hard drive will then be re-formatted. Authorised software will be installed and the data files re-instated in the My Documents folder. The School does not accept any responsibility for the loss of any software deleted due to a re-format and re-image.

13.8 Upgraded version of licensed software are available from time to time. Students will be instructed to bring their tablet to the ICT Help Desk in the technology centre to upgrade their software from the school's network periodically

14. SOFTWARE LICENSING CONSIDERATIONS

14.1 Software installed on notebooks purchased through the BPMS Notebook Program is subject to Academic Licensing agreements, and as such, the use of software is restricted to School and student use only. If you leave BPMS, or transfer ownership of your computer to an owner outside the school, you are required by law to remove any software covered by Academic Licensing, The ICT service desk can provide you with details of this software upon request.

14.2 If you have any queries relating to this document, please contact the BPMS ICT service desk via e-mail at ictservicedesk@bpms.co.za, or by phone on (011) 463 9371. The ICT service desk is open from 08:00AM to 05:00PM weekdays (including school holidays but excluding public holidays).

15. INSPECTION

15.1 Students may be selected at random to provide their tablet for inspection for the purpose of determining whether the student's use of the tablet conforms with this policy

16. ACKNOWLEDGMENT

16.1 In accessing the BPMS Network, students, teachers, and parent(s)/guardian(s) agree to be bound by the principles outlined in this policy with regard to the use of e-mail, devices, Internet and network resources.