1. This policy has been drafted in accordance with the provisions of the Constitution of South Africa, 1996; the South African Schools Act 84 of 1996 ('SASA'); the National Education Policy Act 27 of 1996; and the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002.

2. The purpose of this policy is to govern the use of the school's information systems and to set out rules for the appropriate use of information technology, including social media platforms, by staff members and pupils.

3. The school recognises the evolution of social media as a mode of communication, but also realises that to optimise the use of social media, it must be used responsibly.

4. This policy applies to all users of the school's and information systems. It also applies to the expression of opinions and comments by staff members and pupils on social media that may in any manner be linked to the school.

5. The school respects the individual privacy of staff members and pupils. However, this privacy does not extend to the use of equipment, resources or supplies provided by the school.

6. The school may intercept any communication that is conveyed through the school's information systems or social media platforms.

Definitions

7. Information systems – the systems consisting of the network of all communication channels used within the school.

8. Social media – the means of interaction among people during which they create, share and exchange information and ideas in virtual communities and networks. Social media include text, audio, video, images, podcasts and other multimedia communications.

9. Systems hardware – any mechanical or electronic device linked to a computer system, including the central processing unit and added or additional devices such as printers and external disk drives.

10. Systems software – computer software designed to operate and control computer hardware and to provide a platform for running application software.

General

11. The school's computer and communication systems are intended for official school purposes only.

12. Incidental personal use by staff members is nonetheless permissible if the use
    a. does not consume more than a trivial amount of school resources;
    b. does not interfere with staff productivity;
    c. does not detract from any school activity, and
    d. does not cause distress, legal problems or morale problems for the school or for other staff members or pupils.

13. All systems hardware and software are the property of Pinelands North Primary School.

14. The school has legal ownership of the contents of all files that are stored on its computer and network systems, as well as all messages that are transmitted via these systems.

15. The school reserves the right to access all information on its computer and network systems without prior notice.

16. The school reserves the right to audit systems on a periodic basis to ensure compliance with this policy.

17. The school may at its own discretion examine, move or delete files, including electronic mail (e-mail), for purposes of system maintenance or if the files are determined to be disruptive to the system or its users, either intentionally or unintentionally.

18. The school provides no warranties of any kind, whether expressed or implied, for the IT resources and services it provides.

19. The school will not be responsible for any damages suffered while on its system, including loss of personal data due to system outages or irresponsible use.

20. The school is not responsible for offensive material obtained by any user using the school's information systems.

21. Each staff member shall be granted access to information as needed to perform his or her assigned function, but shall not be given access to information otherwise requiring protection unless and until such access is needed and formally authorised. Authorised users are responsible for the security of their passwords and accounts.

22. The parent representatives of each class shall have access only to the e-mail addresses of the parents of the class they represent.

23. All school information systems privileges shall be promptly terminated when a staff member ceases to provide services to the school, or when a pupil leaves the school. The school reserves the right to revoke any user's privileges at any time.

24. Conduct that interferes with the normal and proper operation of the school's information systems, adversely affects the ability of others to use these information systems, or is harmful or offensive to others shall not be permitted.

Prohibited activities and behaviour

25. The following activities and/or behaviour are prohibited:
    a. Copying material bearing copyrights or patents, without proper licensing or authority
    b. Using the school's information systems for political lobbying, personal gain or commercial purposes
    c. Copying or removing software from the school's computers
    d. Downloading material from the internet that is not related to official school activities or business
    e. Installation of system hardware or software by unauthorised personnel
    f. Loading onto official school computer equipment unlicensed software, privately owned software, games, public-domain software, and freeware, shareware or demonstration software without prior written consent from the governing body or school official to whom supervising authority has been delegated.
    g. Viewing or transmission of any material that violates any national, provincial or international law
    h. Use of school information systems to gain unauthorised access to any system or data
    i. Accessing, downloading, storing or transmitting obscene material through the school's computer network system
    j. Using the school's information system for offensive material or computer harassment.

26. The following constitutes computer harassment:
    a. using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures or other materials, or threats of bodily or psychological harm to the recipient;
    b. using the computer to contact another person repeatedly with the intent to annoy, harass or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease;
    c. using the computer to contact another person repeatedly regarding a matter about which one does not have the legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease;
    d. using the computer to disrupt or damage the academic research, administrative or related pursuits of the school or another person;
    e. using the computer to invade the privacy, academic or otherwise, of another, or the threatened invasion of privacy of another; and
    f. material containing sexist, racist and/or violent content.

27. The following acts of 'cyber misconduct' are prohibited:
    a. 'Cyber-loafing' and the abuse of the employer's resources – Staff members and pupils

are prohibited from using the school's IT resources for private purposes during or outside school hours beyond the incidental personal use by staff members as described in section 12 of this policy.

b. Creating disharmony and distributing offensive or abusive material – Staff members and pupils may not circulate information that is racist, defamatory, sexist or pornographic. This constitutes gross misconduct.
c. Derogatory statements – Staff members and pupils may not post or distribute derogatory and offensive messages about the school, its staff or pupils. An offender may be found guilty of bringing the school into disrepute, which could lead to disciplinary action or legal action for defamation.
d. Breach of trust – Staff members and pupils may not use the school's information, information systems or social media platforms in a way that breaches the school's trust.

Use of Internet

28. Internet access shall be granted to employees who have formally applied for such access and have a legitimate need for it.

29. All internet connections shall be via the approved internet service provider of the school. Any other connections are prohibited.

30. Internet use is a privilege, which constitutes the acceptance of responsibilities and obligations that are subject to government policies and laws as well as the policies of the school.

31. Internet use must be legal, ethical and respectful of intellectual property, ownership of data, systems security mechanisms and individual rights to privacy and freedom from intimidation, harassment and annoyance.

32. Users shall be subject to limitations on their internet use, as determined by the appropriate supervising authority.

33. To protect the school from profane material and to minimise the use of bandwidth, all internet use shall be monitored by web content filtering software.

34. Content filtering software shall prevent users from connecting to certain websites that do not relate to school business. Websites that contain sexually explicit, profane and other potentially offensive material shall be blocked via the firewall.

35. At any time and without prior notice, school management reserves the right to examine web browser cache files, web browser bookmarks and other information that is stored on or passing through the computers of the school. Such access by school management is aimed at ensuring compliance with internal policies and assisting with internal investigations and the general management of the school.

Use of E-mail

36. The school does not guarantee privacy or confidentiality of any e-mail.

37. Use of e-mail to violate this or any school policy is prohibited.

38. Any use of e-mail that does not reflect the image and reputation of the school is prohibited.

39. The user bears sole responsibility for all transmissions using his/her assigned e-mail address.

40. Concealment or misrepresentation of names, addresses or affiliations in e-mail is prohibited.

41. Use of e-mail for private commercial purposes is prohibited.

42. Use of e-mail that is threatening, offensive or intended for purposes of harassment is prohibited.

Use of Social Media

43. The social media sites approved by the school may only be used for official purposes.

44. Postings must be kept legal, ethical and respectful.

45. Staff members and pupils may not engage in online communication activities that could bring the school into disrepute.

46. If any staff member, pupil or parent posts a remark, photo or video on any social media platform that may harm the reputation of the school, and affiliation to the school is identified, known or presumed, such staff members or pupil will be subject to disciplinary and legal action. Legal action may be taken against a parent who jeopardises the school's reputation.

47. All information that is published on social media sites must be accurate, and confidential information may not be disclosed.

48. Personal details of staff members, pupils and parents may not be disclosed.

49. Staff members, pupils and parents should take note that the school may from time to time share photos on social media sites that were taken during official school activities. People may then be 'tagged'. Users of these social media sites are advised to check their security settings if they prefer to review postings in which they were 'tagged'.

50. Staff members and pupils are advised to block other users who they do not know or do not want to be associated with, from accessing their profiles.

51. The school does not accept any responsibility or liability for weak security settings on the social media profile of any person associated with the school.

52. Copyright laws must be adhered to.

53. Only the official approved logo of the school may be used.

54. Statements to the media must first be approved by the Governing Body or school official to whom this task has been delegated.

Acceptance of Personal Responsibility

55. Any person who uses an information system of the school shall be responsible and accountable to follow recommended procedures and to take all reasonable steps to safeguard the information handled by the system as well as any assets involved.

56. The user is solely responsible for all materials viewed, stored or transmitted from school-based computers.

57. The school expects users to comply with all school rules. Failure to do so may result in the suspension or revocation of a user's access privileges as well as disciplinary measures, including the possibility of civil and/or criminal liability.

58. Staff members who fail to adhere to this policy will be subject to disciplinary proceedings in terms of the grievance and disciplinary procedure of the school and/or procedures conducted by the Department of Basic Education.

59. Pupils who fail to comply with this policy and the school's Code of Acceptable IT Use will be subject to the school's code of conduct and disciplinary procedures for pupils.

June 2014