BANKSTOWN WEST PUBLIC SCHOOL

Social Media Policy

As at July 2014

1. Policy Statement:
   1.1. The internet provides an opportunity to enhance students' learning experiences by providing access to vast amounts of information across the globe. Online communication links students to a collaborative learning environment and is intended to assist with learning outcomes. Today's students are exposed to online communication tools and the internet in their community. They have the right to expect secure access to these services as part of their learning experiences.
   1.2. Access to internet and online communication tools at school will assist students to develop the information and communication skills necessary to use the internet effectively and appropriately. Responsible use of the services by students, with guidance from teaching staff, will provide a secure and safe learning environment.

2. Audience:
   2.1. The students, parents and staff of Bankstown West Public School

3. Context:
   3.1. Use of web 2.0 technologies/social media is increasingly part of everyday online activities.
   3.2. DIGITAL CONDUCT – The focus is on the values of a good digital citizen, how to be one, and the idea that online environments are communities that users are helping to shape for the future.
   3.3. DIGITAL FOOTPRINT – This domain includes understanding the trail left by activity in a digital environment, recognising that nothing in the online world is confidential and what is published online can last for years.
   3.4. DIGITAL RELATIONSHIPS – This includes when and how to restrict access to or limit personal information about self and others, the responsibility to protect others from humiliation, and how to report abuse online.
   3.5. DIGITAL HEALTH and WELLBEING – This domain looks at balancing time online with relationships with friends and family in the real world and includes occupational health and safety issues, and responsible and no-risk gaming.
   3.6. DIGITAL LAW – The focus is on productive use of online resources for both study and entertainment while understanding the potential consequences of downloading content and plagiarism.
   3.7. DIGITAL FINANCIAL LITERACY – This domain includes how to be an aware consumer in the digital economy.
   3.8. CYBERBULLYING – All online users should understand what constitutes cyberbullying and what they can do about it, be active in preventing cyberbullying and understand that even one-off hostile cyber actions can have a negative widespread impact due to the rapid dissemination and relative permanency of the message sent.
   3.9. Related Information:
      This policy must be read in conjunction with the school's *Student Use of Mobile Devices Policy*.
      This policy must be read in conjunction with the document *Digital Citizenship Agreement.*
      For further information, see What Staff Need to Know About Social Media and technology: https://detwww.det.nsw.edu.au/policies/technology/communication/techguide.pdf
      Also, Social Media Guidelines:
      https://detwww.det.nsw.edu.au/policies/technology/communication/socmed_guide.pdf

4. Responsibilities:
   4.1. The principal is responsible for the implementation and review of the policy.
   4.2. The teachers are responsible for implementation of the policy and monitoring of student use.

4.3. The parents are responsible for ensuring they are overseeing their children's responsible use of social media.

4.4. The students must use internet and online communication services in a responsible manner.

4.5. Students have the responsibility to report inappropriate behaviour and material to their teachers.

4.6. Students must abide by the DEC's conditions of acceptable usage, and the Bankstown West's *Digital Citizenship Agreement.* Students should be aware that a breach of the policy/agreement will result in disciplinary action in line with the school's discipline policy.

4.7. Access and Security:

    4.7.1. Students will:

- ensure that communication through internet and online communication is related to learning, as appropriate.
- keep passwords private, and change them when prompted, or when known by another user.
- use passwords that are not obvious or easily guessed.
- never allow others to use their personal accounts.
- log off at the end of each session to ensure that nobody else can use their account.
- promptly tell their supervising teacher if they suspect they have received a computer virus or spam or if they receive a message that is inappropriate or makes them feel uncomfortable.
- Never provide personal information of themselves or others to any other user.
- never forward emails or other messages containing a message that was sent to them in confidence or spam.
- never send or publish: unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments; threatening, bullying or harassing another person or making excessive or unreasonable demands upon another person.
- be aware that all use of internet and online communication services can be audited and traced to the accounts of specific users.

4.8. Privacy and Confidentiality

    4.8.1. Students will

- never publish or disclose the email address of a staff member or student without that person's explicit permission.
- never reveal any personal information including full names, addresses and telephone numbers.

4.9. Intellectual Property and Copyright

    4.10.1 Students will:

- never plagiarise information and will acknowledge the author and source of information used.

5. Monitoring and Evaluation:

5.1. The principal is responsible for the implementation and review of this policy.

5.2. Students will report any internet site accessed that is considered inappropriate.

5.3. Students should be aware their emails are archived and web browsing is logged. These records are kept for two years.

6. Contact:

6.1. The principal via the admin office or on 9790 6158.