Published:2019
Reviewed: 2020
Next Review: 2023

ASHBURY PUBLIC SCHOOL COUNCIL
Internet and Mobile Devices Policy

RATIONALE

This policy reflects the NSW Department of Education Online Communication Services: acceptable usage for school students policy which can be found at: https://education.nsw.gov.au/policy-library/policies/online-communication-services-acceptable-usage-for-school-students?refid=285859

POLICY STATEMENT

The internet provides opportunities to enhance students ' learning experiences by providing access to vast amounts of information across the globe as well as opportunities to create content in creative ways that demonstrate learning. Online communication links students to a collaborative learning environment which can 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 at school.

The use of the internet in learning should:

- enhance students' learning opportunities and outcomes in all learning areas from Kindergarten to Year 6
- assist students to develop the information and communication skills necessary to use the internet effectively and appropriately
- reflect key community values

IMPLEMENTATION

At enrolment parents and carers are given the opportunity to give consent for their child to access the Department's Kidspace Portal. Within this portal students are given access to secure email, a range of Google Apps for Education, Microsoft Office 365 and Oliver, a library search terminal. By supporting students to make effective use of technology and the internet in their learning, we allow them to learn the values, behaviours and skills required to contribute meaningfully in an increasingly online world while ensuring that they have the knowledge and skills to successfully manage the challenges of the internet.

Keeping Students Safe Online

Students should use the Department's internet service safely, effectively and responsibly. Keeping students safe online is the responsibility of all members of our community. To this end the school commits to working with parents to jointly understand the issues around safe internet access for students.

All devices that access the internet through the school's wired or wireless internet connections are subject to Department of Education filters. These filters operate at a range of levels and allow staff to access a wider range of websites than students. School staff have the ability to report inappropriate sites and have them blocked for students. Alternatively, they can apply to have restrictions lifted for some sites.

Internet use is monitored by the Department and devices can only access the internet through authenticated user accounts by inputting a username and password.

Mobile Devices

Students whose parents wish them to bring a mobile phone to school are required to sign a contract at the start of the school year. They are expected to switch their phone off when they enter the school, check it into the school office for safe keeping and only switch it back on as they leave school in the afternoon.

Students bring mobile phones to school at their own risk, the school and school staff members will not accept any responsibility for any loss or damage to mobile phones or for investigating loss or damage.

The use of mobile phones, handheld mobile devices and smart watches during school hours is not permitted. This includes on excursions, sport activities and camps. Should students need to phone their parents or carers during the day, office staff can assist them to do so. In the case of emergencies, parents and carers can contact their children via the school office. For these reasons we discourage students from bringing mobile devices to school.

If a mobile phone is used on school grounds during school hours the phone or device will be given to the Principal and parents will need to collect the phone from the school.

Students must not lend a phone to another student for use as a phone, for text messaging or use as a camera or video recording device. The student who owns the phone will be held responsible for its use.

Electronic Communication

If parents and carers provide consent at enrolment, students are issued with a Department of Education email address. The use of this email address is for educational purposes only and all communication via email should be respectful.

Students should be aware that a breach of this policy may result in disciplinary action in line with the school's discipline policy and students may be blocked from accessing email, the internet or blocked completely from using electronic devices at school. Students, parents and teachers should be aware that bullying or threatening behaviour that takes place online outside of school hours can still be dealt with as a school matter under the school's discipline policy if it involves students at the school.

Permission to Publish

At the start of each year, the school seeks permission to publish student work and images from parents and carers through a note that is sent home (see appendix 2). Class teachers keep a register of permissions to publish for their class and the office also enters this information into a student administration database.

When publishing student work or images of students, wherever possible, teachers should avoid publishing the personal details of students. First names, not surnames should be used.

Specifically, teachers should avoid publishing any 3 of the following identifiers together:

- The student's name
- The student's image
- The school's name
- The student's class

Consideration needs to be given to the location on which the work or images will be published. For example, if photographs of students are being published on the school website, the student's name should not be used as 3 identifiers will be published. Extra care should be taken when publishing photos as the school name may be identified on school uniforms.

There may be occasions where 3 or more identifiers are required in order for the published content to make sense. In this case the child's parent or carer should be contacted for approval before the content is published. An example of such a situation might be when an individual student has represented the school at a high level. The school may ask the child's parent for permission to publish their photograph next to text which details the child's first name in the school newsletter.

RESPONSIBILITIES

The teacher's role is to:

- Provide a safe learning environment for students. Appropriate supervision by teachers should be provided whenever students gain access to the internet at school. Wherever applicable as a component of class learning, teachers should remind students of the concepts of digital citizenship when engaging with learning online.
- Support students to use the internet in an appropriate, positive manner and to understand their responsibilities with regard to copyright.
- Where possible, carefully select sites before including them in class learning. This may include taking measures to control advertising.
- Communication through electronic means should be treated as a form of publishing and teachers should ensure that content is appropriate for transmission. Equally transmissions received by students should be monitored. When a class sets up a public blog, wiki or website teachers are required to act as the administrator and approve, monitor or reject content before it is uploaded.
- No access to the internet will be allowed during lunchtime when the children are inside the classroom due to wet weather. Other factors relating to supervision include the careful location of computers and classroom management strategies. The challenge for teachers is to assist students to develop the knowledge, skills and attitudes necessary to locate, select and use information from the internet for curriculum purposes. The internet should be used as a research or publishing tool and not simply for entertainment purposes. Therefore students should only be allowed access for a specific educational purpose.
- Provide details of students email addresses and can assist parents by resetting passwords to parents so that parents can supervise their child's use of email.

Parents'and carers roles are to:

- Monitoring your child's behaviour online at home. Spend time with your child discussing the sites they use online as part of a regular, ongoing conversation. Reassure your child that they can tell you anything, without fear of losing the device or internet access.
- Monitoring your child's electronic communication between peers. Help your child to understand the usefulness of electronic communication and the importance of being respectful when sending messages.

- Discussing strategies that your child could use if they were upset or felt uncomfortable about something encountered online. If they get a message or email that's threatening or rude, they should 'STOP, BLOCK, TELL'. This entails telling your child to stop responding to the abuse and then block those people sending threatening or rude messages if they continue. Let your child know that if they are being bullied, or know someone else who is, they should tell a trusted adult.
- Reporting instances of bullying to your child's class teacher.
- Ensuring that internet devices are used in a central, communal location at home, not in a private space such as a bedroom.
- Setting time limits around technology use at home.
- Discussing the importance of keeping personal information private online and set in place agreed levels of personal information that your child can share.
- Reinforcing 'stranger danger' messages and encouraging your child to question whom they trust online. There is the chance that people may not be who they say they are.
- If you suspect your child has been contacted by a predator, save a copy of the chat log (or whatever form the contact takes) for evidence. Call Crime Stoppers 24-hour line 1800 333 000 to report it to the Police.
- Encouraging your child to think before they post information online. They should understand that once information is posted, it can be difficult to remove it.
- Reminding your child the importance of keeping passwords secret.
- Ensuring that your child's online profiles are set to private so that their personal information is kept secret.
- Ensuring that your child complies with minimum age standards set in the user agreements of social media sites before joining them.

The student's role is to:

- Report inappropriate behaviour and material to their teacher or another responsible adult as soon as possible.
- Abide by the conditions of acceptable usage. They are required to agree to the acceptable usage policy each time they log on.
- Each year students and parents are required to sign a contract for the responsible use of ICT at school (see appendix 1). Students in Years 3 to 6 and their parents are required to sign this contract, while students in Kindergarten to Year 2 have their parents sign it to state that they have discussed the conditions of the contract with their child.

MONITORING, EVALUATION AND REVIEW

This policy will be reviewed in 2021 and again every 3 years after that.

SUPPORTING DOCUMENTS

The following sites may be of use to parents and carers in keeping children safe online.

School A to Z Pages:

- Technology - http://www.schoolatoz.nsw.edu.au/en/technology
- Keeping kids safe online - http://www.schoolatoz.nsw.edu.au/technology/cybersafety/keeping-kids-safe-online
- Cybersafety tips every parent should know - http://www.schoolatoz.nsw.edu.au/technology/cybersafety/cybersafety-tips- every-parent-should-know
- Raising good digital citizens - http://www.schoolatoz.nsw.edu.au/technology/using-technology/raising-good-digital-citizens

Australian Government Office of the Children's eSafety Commissioner

- https://www.esafety.gov.au/

Kids Helpline

- https://kidshelpline.com.au/kids/tips/staying-safe-online/