PULTENEY

B4….Responsible use of ICT Policy

1. Statement of Purpose

Pulteney Grammar School provides its community of learners – students and staff with powerful tools that both support and enhance teaching and learning. These tools or ICT infrastructure include both the physical and wireless network, virtual learning environments, email, cloud storage solutions, other web-services and access devices including, but not limited to laptops, tablets and phones. Devices can either be School owned or personal, bring your own device (BYOD).

There is a responsibility for all members of our learning community to interact with these devices and infrastructure in a way that is consistent with Pulteney Grammar School's values and Learning and Performance Culture.

2. Scope

These guidelines covering the Responsible use of ICT apply to students and staff.

3. The Responsible use of ICT involves

- Using devices and network services for authorised work which is work that is lawful, educational, research, preparation or other school related work.
- Student use of devices (including mobile phones) is at the direction of their teachers and as per the statement under the heading 'Student use of Mobile Phones'.
- Devices being handled responsibly, with care and secured when not being used.
- Respecting Intellectual property and copyright.
- Ensuring that students and staff have an appropriate back up strategy.
- Devices are brought to school each and every day, fully charged.

Approved by Executive June 2017
Date for revision June 2019
Policy developer: Director Learning Technologies
External sources: Protective Practices – for staff in their interactions with young people and children, DECD Social Media Policy
Version: 2

- For students the charger should remain at home.

- Insurance cover should be confirmed for any non-school devices brought to school.

- Devices (including mobile phones) should not contain any material that is inappropriate for a school setting. This would include material that is racist, sexist, pornographic or related to illegal activities.

- Respecting other users and their wellbeing in regard to the communication services (email, instant messaging, and social media). These should not be used to send offensive material, harass, make inappropriate comments or propagate spam.

- Allowing network and communication services and monitoring systems to run as intended.

- Being a responsible digital citizen by maintaining responsibility for your online safety, passwords and device security. Furthermore, not disclosing the personal details of other users, including photographs, addresses, and phone numbers on any site.

- Not filming, photographing or recording of others without their knowledge and permission.

4. Storage and Backups

Students and teaching staff are responsible for their own data management. This includes the storage of data on the device and the backup of that data that they should make. Backups should be done on a regular basis.

All other staff should save their work to the appropriate network or cloud location, and not on their local machine. The School will back up data from the network locations for administration staff. Staff should undertake a regular review of files in line with the Archiving Policy (C17) and delete or archive files as required.

The School provides a cloud based solution, to students and staff through Office 365/OneDrive that may be utilised.

Students and staff should select a suitable back up strategy which is right for them. These may involve an online service such as OneDrive (recommended and provided), iCloud, Google drive or Dropbox. Students may also choose to purchase an external hard-drive from local retailers.

Students, including those in Year 11 & 12 are advised that the loss of significant work can have adverse consequences for student assessment.

The eServices staff can advise on suitable strategies but accepts no responsibility for data loss.

5. Monitoring of network and communication services

The digital services provided by the School including email, internet use, digital learning environments, and School based social media are monitored by the School to ensure usage is compliant with policy. The monitoring of these services is an accepted and justified means of limiting misuse.

6. Internet & email Access

Access to the Internet is monitored through a commercial filter and inappropriate sites are blocked. All internet use is monitored and electronic records kept of all sites visited. Attempts to visit blocked sites are also recorded. **The use of software to circumvent the School's security and monitoring abilities, is not permitted, this includes the Virtual Private Networking (VPN) utilities.**

The School provides staff and students with an email address, which should be used for School purposes only. Should staff or students wish to use email for personal reasons, then they should create a separate email address through the home Internet Service Provider (ISP) or through a web service such as Hotmail.

The School has a high bandwidth connection to provide Internet access across the campus. Students are reminded that the use of the internet should be for educational or curriculum activities only. Downloading of games, music files (.mp3), torrents, video clips and software is not permitted and in many cases such downloads are illegal as they may breach Intellectual Property and Copyright.

7. Intellectual Property, copyright and academic integrity

All users of Pulteney Grammar Schools' ICT infrastructure are reminded of their responsibility to respect the intellectual property and copyright of others. Federal legislation relating to Digital Rights Management (DRM) makes it illegal to download and / or distribute material (music, games, movies etc) that is copyright. As a community of learners we also need to uphold the ideal of Academic Integrity – that is we should not knowingly submit work of others, including material sourced from the internet, as our own. This is known as plagiarism. Correctly referencing this material and acknowledging sources complies with the academic integrity that we as a community seek and respect.

8. Social Media use by Staff – Protective Practices

This section, for the most part, has been taken from the DECD Social Media Policy (2015).

Social Media can be a very positive experience for users; and the School is looking 'to establish a culture of transparency, trust and integrity in social media activities and to encourage the integration of social media into our teaching and learning environments'.

Section 8 of the Responsible use of ICT policy has been established to assist staff members to use social media to:

- Engage internally with staff or with the wider community as a communications tool
- Showcase children and students' work
- Integrate with, and facilitate teaching and learning
- Administer social media platforms in an authorised capacity, or make contributions in a professional capacity on education-related issues.

Professional use of social media

Staff members are responsible for maintaining a professional role with students. This means establishing clear professional boundaries with students that serve to protect everyone from misunderstandings or a violation of professional relationships.

When establishing or using a School or professional social media platform, for school activities, staff must:

- Have approval from their direct line manager and the Deputy Principal Learning & Teaching.

- Be aware of the specific social media channels and etiquette and understand the views and feelings of the target community.

- Ensure all material published is respectful of all individuals, the School and/or the specific social media site.

- Not publish any material that is offensive, obscene, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, breaches a Court Suppression Order, or is otherwise unlawful.

- Ensure that all content published is accurate and not misleading.

- Ensure all information posted or comments made are appropriate to the individual's area of expertise and authority, does not breach any confidentiality guidelines, and that unless specifically given permission to do so a person is not the first to make a significant announcement.

- Ensure that comments on their social media about the School workplace, colleagues or students or young people, if published, would not cause hurt or embarrassment to others, risk claims of libel, or harm the reputation of the school, their colleagues or students and young people.

- Ensure that information and images of them, available on both their personal and/or professional social media, represent them in a light acceptable to their role in working with students and young people.

- Respect copyright laws and attribute work to the original source wherever possible.

- Protect personal details.

- Use School branding in accordance with the Schools' Style Guide.

- Ensure any young people involved understand the rules of operation of each social media site, and measures are in place to protect them from any potential risks.

Most importantly, staff must not have children or young people in their education community, that they are not directly related to, as 'friends' or 'connections' on their personal social media sites.

Staff need to be aware that by being connected to students who are their direct relations (children, nephews & nieces) will potentially allow other students to access information from their personal social media **and** will also allow you to see through your direct relations, the social media status of students. **This then extends the duty of care to those students**.

Social Media use by children and students

- Your behaviour online should be no different to your in person or face to face behaviour. Consequences may apply, in accordance with the Bullying and Harassment policy for inappropriate behaviour.

- Think before you click. Once you have posted or uploaded your comments, photos or videos – they are there permanently. You need to think about your 'digital reputation'- by asking; is what I am posting going to reflect on me positively or negatively?

- Material that you upload may also be used by others in ways that you had not intended.

- If you are the recipient of unsuitable material or are being bullied online, do not respond, but seek assistance from a trusted adult and do keep the material as evidence.

- Protect your privacy and that of your family and friends by not posting personal details such as phone numbers, addresses and ages.

- Check your social media profile settings to ensure they are set to private, thus restricting information available to strangers.

- Accept friend requests from people you can verify.

- Students are not permitted to seek teachers as friends.

9. Student use of Mobile Phones

Our statement around the use of mobile phones is responsive to the growth in responsibility and potential educational use by our students across our sub-schools. **It is not an expectation that students bring mobile phones to school.**

Kurrajong students are not to bring mobile phones to school. If students need to contact their parent, the Personal Assistant to the Head of Kurrajong or the students' classroom teacher will contact the parent directly. If parents need to contact their child, they can do this by phoning the Kurrajong Office. The Personal Assistant to the Head of Kurrajong will directly pass this message on to the student.

Prep students are permitted to bring mobile phones to school, however, they must be turned off as students enter the School, must be placed and remain in school bags and may be turned on once outside the school gate. The School accepts no responsibility for the security of these devices. Phones are not to be taken in to the yard. If, for any reason, a student needs to make a phone call, the student can obtain permission from a teacher and make a call on the class phone or the phone at the reception desk in the Prep School.

Students of both the Middle School and *one ninety* are permitted to bring mobile phones to school and to use them for educational purposes, with the permission of and under the direction of their teachers. This will be at the discretion of the individual teacher. Communicating with other students through voice / sms or in app functionality is not permitted during class-time, unless it is directly related to a school learning activity and with the permission of the teacher. Students are discouraged from using their phones during break times so as to promote positive social interactions and physical activity and provide a break from "screen time".

10. Expectation

The School requires and expects compliance with this policy. Any breach many lead to disciplinary action up to and including termination of employment or enrolment, depending on the seriousness of the circumstances and consistent with any School disciplinary and counselling policies.

PULTENEY

11. Disclaimer

The School accepts no responsibility for any damage or loss arising directly or indirectly from the use of any ICT service or infrastructure or for any consequential loss or damage. The School makes no warranty, expressed or implied, regarding the services / facilities offered or their fitness for any particular purpose.

A commercial filter is used on the internet connection to prevent access to inappropriate sites. However, no guarantee can be made that new sites will be blocked immediately.

While reasonable care, consistent with good business practice and aligned with the School's Privacy Policy (C13), is taken, the School does not guarantee the confidentiality of any data stored on any service or facility or transmitted through any network. **The School reserves the right to examine or copy files or data from any of its storage devices to maintain a secure, efficient and effective ICT environment or if an investigation into alleged misuse of the School's infrastructure and services, is required.**

12. References

Protective practices for staff in their interactions with children and young people Guidelines for staff working or volunteering in education and care settings (revised 2011), Department for Education and Child Development, viewed 26 April, 2017, < https://www.decd.sa.gov.au/doc/protective-practices-staff-their-interactions-children-and-young-people>

Social Media Policy, 2015, Department for Education and Child Development, viewed 26 April, 2017,
< http://www.saasso.asn.au/wp-content/uploads/2016/03/Decd-Social-Media-Policy.pdf >

13. Responsibilities

Director Learning Technologies	Writing and review of policy.
Executive	Policy approval
Staff & students	Are responsible for adhering to this policy and referring any questions to the Director Learning Technologies or the Information Technology Systems Manager. For staff this policy should be read in conjunction with the Pulteney Grammar School Staff Digital Devices Policy (D7) and the Pulteney Grammar School Child Protection Policy (C3).

14. Version Control

Version	Date Released	Approved By	Amendment
1.1	November 2015	Executive	Responsible use of ICT Policy rewritten
2	September 2017	Executive	Moved Student use of Mobile Phones from section 3 to section 9. Added to section 6, 'The use of software to circumvent the School's security and monitoring abilities, is not permitted, this includes the Virtual Private Networking (VPN) utilities.' Have also added a distinction that School email address should not be used for private email. Updated links to external sources. Included relevant internal policy numbers C17, D9. Changed terminology from IT Helpdesk to eServices. Changed 'When posting' to When establishing and using (section 9 professional use of Social media) Added the term connections alongside friends in social media section.

Approved by Executive June 2017
Date for revision June 2019
Policy developer: Director Learning Technologies
External sources: Protective Practices – for staff in their interactions with young people and children, DECD Social Media Policy
Version: 2

			Added to section 9, ‘that it is not an expectation that mobile phones are brought to school.’ Further the term Middle School has been removed from the last sentence (so as to encompass both MS and 190 students) Have introduced section 10 – Expectation on compliance with policy. Have referenced the Privacy Policy (C13) in section 11. Also, added ‘or if an investigation into alleged misuse of the School’s infrastructure and services, is required’.