Appendix 3 - Digital Device Policy

1. Purpose and rationale

1.1 Melville SHS supports the philosophy of using ICT based pedagogy and approved technologies to support the teaching and learning program in the school

1.2 Melville SHS allows staff, students and parents to access the school network to use online services for educational purposes with school owned resources and approved personally owned devices

1.3 The approved personally owned student digital device must be an up-to-date iPad or MacBook. The device must be able to receive IOS or MacOS updates to maintain its security status

1.4 Mobile phones are not approved devices and students should not connect mobile phones to the school Wi-Fi at any time. (See the Student Mobile Phones in Schools Policy)

2. Responsibilities

2.1 The School

• As a Department of Education site, the school uses site monitoring and filtering software to filter inappropriate content
• The Department also applies monitoring software for email communications to ensure that content of emails complies with Department policies
• The school uses software to monitor student activities on the network to ensure compliance with this policy
• The school will offer learning opportunities for staff and students to develop digital literacy
• The school will offer Connect workshops for parents
• Limited printing facilities will be available to students. Printing charges apply, and students are advised to print preview, edit on screen and submit work digitally whenever possible

2.2 Teaching Staff

• Teaching staff will support students' development of digital literacy, digital citizenship and cyber safety with a range of learning opportunities embedded in the curriculum
• Teaching staff use Connect for curriculum management and will provide guidance and instruction to students to access this resource
• Teaching staff will maximise learning opportunities that facilitate the use of the digital device, Microsoft 365 and Connect to support and enrich the curriculum, while considering varied instructional needs, abilities and developmental levels of students

2.3 Students

• Students must bring their iPad or MacBook to school every day, without the expectation that it will be used in every class. Students should utilise the resources on the device such as the calendar to maintain their study plan and explore apps and programs that will support their individual learning journey
• Students have responsibilities relating to use of online services and use of their personally owned device while at school as outlined in this policy
• Students will not use a mobile phone as a digital device in the classroom or at school as outlined in the Student Mobile Phones in Schools Policy, it is 'Off and away all day'
• It is the responsibility of the student to read, understand and acknowledge school policies and abide by these at all times to maintain network access
• Students acknowledge the DoE Telecommunications User Policy every time they sign into a school owned desktop and must abide by this whenever on the school network
• The device is always the responsibility of the student. Melville Senior High School cannot be held responsible for any loss, theft or damage. Students should turn on 'Find my iPad' in the Apple ID Settings and unless attending a physical education lesson, keep their device and any valuables with them at all times

- Students must maintain the device with IOS and MacOS updates when released. When the device can no longer receive updates, it should be replaced to meet requirements for connection to the school network
- Backing up of work is the student's responsibility. Students can utilise the storage space provided in OneDrive as part of their Microsoft 365 account. Students using school owned devices can access their H:// drive storage. Students can also purchase external storage such as a USB or cloud storage to store their work
- Students must use the school provided network to connect to the internet while at school
- Students must not use hot spots or personal dongles at school

2.4 Parents/Caregivers

- The parent/caregiver is expected to provide an approved device (iPad or MacBook) for each child attending Melville SHS
- It is the responsibility of the parent/caregiver to read, understand and acknowledge school policy and convey the importance of this to their child
- The parent/caregiver accepts responsibility for their child's use of any digital device and monitors their child's compliance with the expectations outlined in this policy
- The parent/caregiver establishes and maintains appropriate virus protection on the student device
- The device is always the responsibility of the student and the parent/caregiver accepts that Melville Senior High School cannot be held responsible for any loss, theft or damage
- The parent/caregiver is expected to attend the school to collect their child's device when requested to do so by the school
- The parent/caregiver will familiarize themselves with the Connect platform as this is an 'opt out' process. All student reports are distributed via Connect

3. Acceptable use of school network and digital device

Students will:

3.1 Bring the school approved iPad, MacBook or laptop to school, charged and ready to use **every day**
3.2 Exhibit skills of responsible digital citizenship and demonstrate courtesy, consideration and respect for others
3.3 Utilise the school approved device for educational activities and research as requested by teachers, including Microsoft 365 and Connect resources
3.4 Maintain the Network password and change it on a regular basis (90-day expiration period)
3.5 Report any suspicious activity on their account to the Network Administrator and change the password immediately
3.6 Maintain the Department provided email address (…@student.education.wa.edu.au) and use it for school related communications. Regularly check this email address for Connect notifications
3.7 It is a condition of network access that students agree to the monitoring of all activities including email, internet access, files and documents
3.8 Only use social media in a responsible manner (see Student Engagement Policy)

4. Unacceptable behaviour can result in all network privileges being revoked and appropriate disciplinary action depending on the behaviour

Students will not:

4.1 Access social media on the school network and/or during the school day on digital devices and mobile
phones
4.2 Engage in cyberbullying including, but not limited to; harassment, insults, racial vilification, defamation, personal attack
4.3 Use swear words in any digital communication (obscene language)
4.4 Record, distribute or upload inappropriate images or videos via social media or other platforms of students, parents or staff at any time
4.5 Break copyright laws (see smartcopying.edu.au for student information sheets)
4.6 Participate in and sharing illegal downloads of any material via peer-to-peer networks or any other means

4.7 Access any sites and/or images that are inappropriate/offensive. This includes any site that has any of the following content:
  • Nudity, obscene language or discussion intended to provoke a sexual response
  • Violence – actual or implied or suggestion of violent threats
  • Information about committing any illegal activities
  • Information about making or using weapons, booby traps, dangerous practical jokes or 'revenge' activities

4.8 Reveal their password to anyone except the Network Administrator and/or ICT Manager. Students are responsible for all activity on their account and digital device

4.9 Use another user's password to access the school network

4.10 Trespass into another user's folders, work or files and/or alter them in any way

4.11 Attempt to alter another user's access rights

4.12 Use the school network for any commercial or illegal activities

4.13 Connect their mobile phone or any other unapproved device to the school network **at any time**

4.14 Use a mobile phone in any way that contravenes the Student Mobile Phones in Schools Policy. Mobile phones are 'Off and away all day'

4.15 Play games on school owned devices, unless for educational purposes, under direct instruction by a teacher

4.16 Delete, add or alter any configuration files

4.17 Deliberately introduce any virus or program that reduces system security or effectiveness

4.18 Create any online content that misrepresents Melville Senior High School

4.19 Bypass the school proxy server

4.20 Use or possess any program designed to reduce network security

4.21 Use any other form of connecting to the internet at school. Student activity online requires monitoring

4.22 Use a personal hot spot or dongle while on school premises

5. Digital games in the school environment

5.1 Students must understand that regardless of how they use their digital device at home, at school it is an educational tool and must primarily be used for that purpose

5.2 Melville Senior High School acknowledges that students will install games on their devices, but this must not be done at school. Students must abide by censorship ratings and games or software must be appropriately licensed

5.3 Students must not play MA rated games in shared spaces where younger students can see the content

5.4 Students must not install illegal copies of games

5.5 Students must not play games of any sort on school owned devices, unless it is part of an educational activity, under the direct instruction of a teacher

5.6 Teaching staff may use educational games such as Kahoot and Quizlet to check for understanding as part of their formative assessment.

6. Breach of this policy

6.1 Any breach of this policy may also involve a breach of other school, Department of Education and State and Commonwealth government policies such as:

• Student Engagement Policy (Melville SHS)
• Student Mobile Phones in Schools Policy (Melville SHS)
• Bullying, Discrimination and Harassment Policy (Melville SHS)
• Staff Conduct and Discipline Policy (https://bit.ly/Staffconductpolicy)
• Child Protection Policy (https://bit.ly/DoEChildprotectionpolicy)
• Students Online Policy (/www.education.wa.edu.au/web/policies/-/students-online-in-public-schools-policy)
• Duty of Care for Students Policy (https://bit.ly/DoEDutyofcare)
• Telecommunications Act (www.comlaw.gov.au)

6.2 A breach of this policy will be considered by the principal or their delegate and will be dealt with on a case by case basis. All reports of cyber bullying and other technology misuses will be investigated fully. Sanctions for students may include, but may not be limited to:

- The confiscation and/or loss of electronic device privileges
- The loss of access to the Internet and/or school network
- Detention and/or
- Suspension

6.3 Students, parents and staff should be aware that in certain circumstances a breach of this policy may also mean that a crime has been committed and that breaches of this policy could lead to a criminal investigation by Australian Federal Police, WAPOL and/or the Department of Education Standards and Integrity Directorate.

7. Implementation

7.1 After consultation with staff, students and parents, this policy has been endorsed by the Melville SHS Board. A copy and any future revisions will be made available on the school website and intranet.

Student acknowledgement

If I use the online services of the Department of Education, I must agree to the following rules:

- I will not reveal personal information, including names, addresses, photographs, credit card details and telephone numbers of myself or others when online.
- I will not give anyone my logon password.
- I will not let others logon and / or use my online services account unless it is with the teacher's permission.
- I will not access other people's online services accounts without permission from the teacher.
- I understand that I am responsible for all activity in my online services account.
- I will tell my teacher if I think someone has interfered with or is using my online services account without permission.
- I understand that the school and the Department of Education may monitor any information sent or received and can trace activity to the online services accounts of specific users.
- If I find any information that is inappropriate or makes me feel uncomfortable, I will tell a teacher about it. Examples of inappropriate content include violent, racist, sexist, or pornographic materials, or content that is offensive, disturbing or intimidating or that encourages dangerous or illegal activity.
- I will not attempt to access inappropriate material online or try to access Internet sites that have been blocked by the school or the Department of Education.
- I will acknowledge the creator or author of any material used in my research for schoolwork by using appropriate referencing.
- I will obtain permission from the copyright owner of any materials inserted into my schoolwork before I subsequently reuse it as a portfolio for employment, in a competition or any other uses other than for my private research and study.
- I will make sure that any email that I send or any work that I wish to have published is polite, carefully written and well presented.
- I will follow the instructions of teachers and only use online services for purposes which support my learning and educational research.
- I will be courteous and use appropriate language in all Internet communications.
- I will not use the Department's online services for personal gain or illegal activity (e.g. music file sharing), to bully, offend or intimidate others or send inappropriate materials including software that may damage computers, data or networks.
- I will not damage or disable the computers, computer systems or computer networks of the school, the Department of Education or any other organisation.
- I will be mindful of the possible problems caused by sharing or transmitting large files online.

I understand that:

- I will be held responsible for my actions while using online services and for any breaches caused by allowing any other person to use my online services account;
- the misuse of online services may result in the withdrawal of access to services and other consequences dictated in the School's policy; and
- I may be held liable for offences committed using online services.
- If I am given an online services account and break any of the rules in the agreement, it may result in disciplinary action, determined by the principal in accordance with the Department's Student Behaviour Policy and Procedures.