Administrative Procedures 140 Responsible Use of Technology		
SUN WEST SCHOOL DIVISION Success for all		**Adopted:** June 28, 2011 **Amended:** August 1, 2017
	External References: • Education Act: Sections 85, 87, 109, 175	**Internal References:** • AP 150 Communications - Appendix A – School Websites • Form 140-1 Student Technology Acknowledgement of Understanding

Background

Computer technology is a resource available to all students and staff of the Division that offers vast, diverse and unique resources. Combined with Digital Citizenship education in the classroom, the goal of technology services is to enable both students and educators with the knowledge and tools to use technology safely and effectively in a global society.

The Division supports opportunities for students and staff members to access, evaluate and produce information through responsible use of Division technology and private use of technology in pursuit of student learning and staff professional development.

Procedures

1. School staff are to ensure Administrative Procedures 140 Responsible Use of Technology are understood and adhered to by all students.
2. Passwords and Accounts
   - 2.1 Students shall not share passwords or allow others to use their accounts.
3. Filtering and Monitoring
   - 3.1 The Division employs a content filter to restrict access to inappropriate content. All network traffic is monitored by the division, logging who, when, and what occurs on the network.
     - 3.1.1 Students are not to seek out or visit inappropriate websites. If they do accidentally encounter such a website, they should immediately inform the supervising teacher.
     - 3.1.2 If the Division's content filter is incorrectly blocking access to content, a request may be made to have the resource unblocked by contacting the Helpdesk. The resource will be reviewed before access is allowed or denied.
4. Social Networking and Network Communication
   - 4.1 Use of Division resources to engage in blogging and social networking is acceptable, provided that it is conducted in a courteous, professional and responsible manner.
   - 4.2 Posting of specific personal information or personal information about other people is not allowed.
   - 4.3 Students should under no circumstances meet with an internet acquaintance without parent or guardian permission, and must have adequate supervision.
   - 4.4 Students will not engage in cyber bullying, which is defined as: *"the use of communication technologies to support deliberate and hostile behaviour by an individual or group that is*

intended to harm others". This may include sending hateful or insulting remarks, posting unwanted pictures or other media on the internet, distributing unwanted pictures or media by email or Instant Message, communicating threats, or continuing to contact someone who has requested no further contact.

5. Use of Online Content and Resources

    5.1 Students will respect the rights of content creators and be cognizant of applicable copyright and usage laws.

    5.2 Students will not download or distribute material that they do not have rights to, including but not limited to: movies, music, eBooks, internet video, or software.

6. Use of Division Resources Including Desktop Computers, Laptops, Tablet devices, and Network Equipment

    6.1 Students shall use Division resources for educational purposes

    6.2 Students will not use Division resources for gaming unless associated with an educational outcome and supervised by Division staff.

    6.3 Students will not store personal content on Division servers or devices. This includes but is not limited to personal images, music, or other digital content.

    6.4 Students will not intentionally tamper with or cause physical damage to Division resources.

7. Use of Personally Owned Devices

    7.1 The Division maintains a "Bring Your Own Device" (BYOD) wireless network. Students may access this network using their Division network credentials.

    7.2 The BYOD network is filtered and monitored.

    7.3 Students may not plug personally owned devices into classroom network connections.

    7.4 The Division is not responsible for damage to personally owned devices.

8. Consequences

    8.1 If a student is found to have breached the guidelines laid out in these procedures, or at the direction of a School Principal, The Division IT Manager or designate may prevent access to any computer system at any time as required.

        8.1.1 Student network credentials may be revoked or suspended.

        8.1.2 Access to Division owned computing devices may be removed.

        8.1.3 Access to the BYOD wireless network may be revoked or suspended.

    8.2 The School Principal will make the final decision on what is deemed inappropriate use by students.