GENERAL SCHOOL ADMINISTRATION

Computer Systems and Network Services – PWCS Responsible Use and Internet Safety Policy

This regulation contains the Responsible Use and Internet Safety Policy of Prince William County Public Schools (PWCS), as authorized in Policy 295, "Standards for Use of Telecommunications and Internet Technologies." This governs the use of all PWCS local area networks, wired and wireless, wide area networks, the Internet/Intranet/Extranet-related systems, all PWCS websites, and all other similar networks. This policy also specifically applies to the use of PWCS computer equipment; software; operating systems; storage media; cloud solutions; web applications; network accounts providing access to network services such as email, messaging, web browsing, and file systems; as well as telecommunication technologies such as telephones, personal computers, cellular phones, personal use devices, facsimile machines, and all other wired or wireless telecommunication devices.

Non-PWCS assets or personal use computer systems are only permitted to connect to the PWCS Guest wireless network, unless explicitly instructed otherwise by the Director of Information Technology Services, or designee. Student or staff use of personal devices in schools or classrooms must comply with applicable federal and state laws, guidelines, regulations of the Virginia Department of Education, and School Board policies and regulations.

To the extent this regulation can apply to other information and telecommunication technologies, it shall be interpreted to apply to them as well. This document supersedes all previous Responsible Use policies and regulations for PWCS.

I. PWCS Instructional Philosophy

PWCS is committed to *Providing A World-Class Education* to meet the educational needs of our diverse student population. The instructional program in PWCS is implemented through a planned systematic approach which outlines the knowledge and skills to be taught in each subject and grade level so that all students are *Future Ready*.

Technology is a valuable tool that supports and enhances the PWCS instructional program by promoting problem solving, critical thinking, analytical, and decision making skills. Students and staff will access, process, and communicate information in a dynamic, integrated, and technological environment.

II. Expectation of Privacy

Employees and students have no expectation of privacy in their use of school computers or internet services, nor does the use of PWCS computers or related venues create an open or limited forum under the First Amendment to the federal or state constitutions. Any expectation of privacy related to the use of student or staff-owned devices is negated by the failure to comply with this regulation or other School Board policies and regulations. The Division retains the right to monitor all computer and internet activity by employees and students, and any information or communications on PWCS computer systems and network services may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Use of PWCS computers, networks, and internet systems is a privilege, not a right, and can be withdrawn by the Division at any time.

III. Acceptable Uses of PWCS Computer Systems and Network Services

It is the general policy that PWCS computer systems and network services are provided for administrative, educational, communication, and research purposes consistent with the Division's educational mission, curriculum, and instructional goals. General rules and expectations for professional behavior and communication apply to use of the Division's computers, networks, and internet services, as do those rules of student conduct set forth in the PWCS "Code of Behavior." Acceptable uses of computer systems and network services include activities that support teaching and learning. Acceptable activities in support of this purpose include, but are not limited to, professional development, administrative communications, grant applications, new project announcements, and student product publishing.

A. Acceptable Use by Employees

Employees are to utilize the Division's computers, networks, and internet services for school-related purposes and performance of job duties. Incidental personal use of school computers is permitted as long as such use does not interfere with the employee's job duties and performance, with system operations, or other system users. "Incidental personal use" is defined as use by an individual employee for occasional personal communications not occurring during instructional time, which use is not otherwise prohibited by this regulation.

B. Unacceptable Uses of PWCS Computer Systems and Network Services

Any infraction of the regulation will not be tolerated and PWCS will act quickly in correcting the issue if the Responsible Use and Internet Safety regulation is not followed. Any user found to have violated this regulation, Regulation 295-2, "Website Development and Implementation," any other applicable School Board policy or

regulation, or applicable provisions of the PWCS "Code of Behavior" and/or Regulation 503.02-1 "Standards of Professional Conduct" are subject to disciplinary measures, up to and including revocation of privileges; student discipline, up to and including expulsion; administrative action; employee discipline, up to and including dismissal; and criminal prosecution under applicable local, state, and/or federal law.

C. Examples of Unacceptable Uses of PWCS Computer Systems and Network Services

The following is a non-inclusive list of examples of unacceptable actions or activities:

1. Any use that is illegal or in violation of other School Board policies or regulations;

2. Violating the rights to privacy of any student or employee;

3. Transmitting, downloading, storing, or printing files or messages (text, sound, still, or moving graphics, or any combination thereof) that are pornographic, or are obscene, as defined at Va. Code §18.2-372, or that use language, sounds, or imagery which is lewd or patently offensive (including "sexually explicit visual materials" as defined at Virginia Code §18.2-374.1), or degrades others (the administration invokes its discretionary rights to determine suitability in particular circumstances);

4. Transmitting, downloading, storing, viewing, or printing files or messages (text, sound, still or moving graphics, or any combination thereof) that are plainly offensive, lewd, vulgar, or are otherwise inconsistent with the curricula and educational mission of PWCS;

5. Harassment by computer, which includes transmitting any material or posting material on any website which is threatening to another person, or which is intended to coerce, intimidate, or harass; material intended to communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, or make any suggestion or proposal of an obscene nature; or material threatening any illegal or immoral act, whether or not such material is transmitted to that third person;

6. The School Division has no legal responsibility to regulate or review off-campus internet messages, statements, postings, or acts, nor those made on campus using student or staff-owned devices in violation of regulations

concerning the use of these devices. PWCS reserves the right to discipline students or employees for actions taken off-campus or using private equipment, which would violate this regulation if occurring on-site or via PWCS hardware, if such actions adversely affect the safety, well-being, or performance of students while in school, on school buses, at school activities, or coming to and from school, if such actions threaten violence against another student or employee, if such actions violate local, state, or federal law, or School Board policies or regulations or the "Code of Behavior," and/or Regulation 503.02-1 "Standards of Professional Conduct," or if such actions disrupt the learning environment, administration, or orderly conduct of the school. The Division may also take appropriate disciplinary measures, up to and including dismissal, for off-campus internet activities which are inconsistent with the professional and ethical standards expected of PWCS employees as "role models" for PWCS students;

7. Copying and/or installing proprietary information, including software, in violation of software licensing agreements and applicable law;

8. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music or videos, and the installation of any copyrighted software for which PWCS or the end user does not have an active license;

9. Using the PWCS network or information contained on the network for personal financial gain, commercial advertising, solicitation or business activity not on behalf of PWCS, unless authorized under Regulation 923-1, "Commercial Advertising," or any illegal activity;

10. Any use for a forum for communicating by email or any other medium with other school users or outside parties to solicit, proselytize, advocate, or communicate the views of an individual or non-school sponsored organization; to solicit membership in or support of any non-school sponsored organization; or to raise funds for any non-school sponsored purpose, whether profit or non-profit. No employee shall knowingly provide names, email addresses, or other personal information to outside parties whose intent is to communicate with school employees, students and/or their families for non-school purposes. Employees who are uncertain as to whether particular activities are acceptable shall seek further guidance from

their Supervisor or the Director of Information Technology Services;

11. Sending mass emails, chain letters, or using messaging platforms, to send messages to school users or outside parties for school or non-school purposes, or otherwise inconsistent with the curricula and educational mission of PWCS without the permission of an administrator;

12. Use of the PWCS asset or PWCS affiliated online account for political purposes, including any use requiring students to convey or deliver any materials that (a) advocate the election or defeat of any candidate for public office; (b) advocate the passage or defeat of any referendum question; or (c) advocate the passage or defeat of any matter pending before the School Board, the Prince William Board of County Supervisors, the General Assembly of Virginia, or the Congress of the United States;

13. Any attempt to bypass security controls to access unauthorized web sites or computer systems;

14. Any attempt to delete, erase, or otherwise conceal any information stored on a school computer which violates these rules, or at any time after being advised by any administrator or supervisor to preserve any materials stored on a school computer;

15. Deliberately trying to degrade or disrupt system or network performance. Such acts will also be viewed as criminal activity under applicable state or federal law;

16. Transmitting or displaying messages promoting the sale of products/ services, except as provided in Regulation 923-1, “Commercial Advertising”;

17. Attempts to modify system facilities, downloading, installing, or transmitting malicious software from email attachments or any other source, illegally obtaining extra resources, or attempting to subvert the restrictions associated with any computer system, computer account, network service, or personal computer protection software;

18. Writing down passwords and storing them anywhere accessible to others or storing passwords in a file on any computer system (including smart phones, tablets, or similar devices) without encryption;

19. Re-posting personal communications without the author's prior consent;

20. Fundraising or links to fundraising information on school/department websites or the PWCS web page, unless explicitly authorized as part of PWCS activities;

21. Sending PWCS proprietary and classified information to unauthorized persons, or posting this information outside of PWCS;

22. Distributing any school interior maps, floor plans, written descriptions of interior floor plans on web pages, camera locations, or other information which could compromise school security;

23. Connecting non-PWCS computer equipment to the PWCS network or computer equipment through means other than the Wireless Guest Network, or the designated Wireless Network approved by the Director of Information Technology Services; and

24. Any content prohibited by Regulation 295-2, "Website Development and Implementation."

IV. Responsible Use of Personally-Owned Wireless Communication Devices

In recognition of the growing importance and utility of wireless communication devices (smart phones, tablets, E-readers, etc.), the use of these personally-owned devices by students and employees will be permitted within PWCS schools and classrooms, provided such use complies with the "Code of Behavior," and/or Regulation 503.02-1 "Standards of Professional Conduct" and with rules established below.

In correlation with Regulation 561.02-1 (where teachers provide for individual differences through the use of varied materials and activities suitable for students with different interests and abilities), principals and teachers will work collaboratively to determine the effective use of, when, and how BYOD is put into practice in their classrooms, and to establish special rules or prohibitions to times and locations of responsible use.

All school and classroom rules will incorporate the following guidelines:

1. Possession of communication devices by students or staff on PWCS grounds is a privilege, not a right, and any staff member or student who brings a communication device on PWCS property consents to these rules and to the

School Division's right to confiscate and/or search such devices as provided in these rules;

2. All devices must be set to silent or vibrate mode, with audible signals disabled during all in-school use;

3. Speaker settings must be turned off. Audio content must be delivered by means of earphones or handsets to prevent any disruption of school activities;

4. Specific safeguards are required to ensure the integrity of academic testing. For each specific testing situation, principals and/or classroom teachers will establish and affirmatively state specific rules governing the use of devices in these instances. For example, the use of a calculator application may be permissible for certain math or science tests, while all communication applications must be disabled; a teacher may determine that all devices must be turned off; or principals and/or Division officials may prohibit the use of devices in all areas of a school during major standardized or periodic exams;

5. Violation of any specific device-use restrictions observed during testing may be deemed as cheating and punishable as such. Any use of electronic communication devices for the transmission or receipt of testing questions, answers, or other protected content will likewise be treated as cheating;

6. Wireless communication devices may be used on school buses provided that the device does not distract the driver, compromise safety, or violate other school bus rules and regulations. Violators are subject to confiscation of the communication device and/or other corrective action;

7. Searches of communication devices may be conducted if the administrator has a reasonable suspicion that it is being used for conduct that is criminal or a violation of the "Code of Behavior" and/or Regulation 503.02-1 "Standards of Professional Conduct," as applicable. Password protected devices are expected to be unlocked to perform searches upon request;

8. PWCS does not assume responsibility for the security of communication and/or electronic devices that are brought onto PWCS property;

9. While on school property, at any school-related activities or while traveling to and from school or any school-related activities, students shall neither take nor display video graphic or still images of a person who is undressed or partially

undressed. Violators may be subject to disciplinary action up to and including expulsion. Under Virginia Code, § 18.2- 386.1, this crime is a misdemeanor if the victim is an adult, but a felony if the victim is under 18;

10. Use of wireless devices while on school property, at any school-related activities or while traveling to and from school or any school-related activities is subject to all terms of the "Code of Behavior" and/or Regulation 503.02-1 "Standards of Professional Conduct"; and

11. The School Division cannot monitor nor be held liable for communications or actions originated on personally-owned devices used on PWCS property.

V. Acceptable Use of 1:1 Student Digital Devices

In-school and take-home use of 1:1 student digital devices (e.g., laptops, tablets) must comply with the rules established in Regulation 426.01-2, "Accounting of Student 'Take-Home' Digital Devices that are Classified as Expendable Property" and Regulation 701, "Code of Behavior," along with the guidelines established by principals and teachers in the school-based implementation of the regulation defining the PWCS Responsible Use and Internet Safety Policy. In so doing, students are responsible for only using PWCS computer systems/digital devices and network services as directed by teachers for the completion of classroom, curriculum-based assignments. By completing the "Digital Device Student Loan Agreement," parents/guardians shall be responsible for ensuring that their students adhere to all established regulations, rules, and guidelines for take-home 1:1 use of digital devices.

VI. Areas of Responsibility

Employees, students, contractors, consultants, temporary employees of PWCS, including all personnel affiliated with third parties, volunteers in PWCS, and all other persons granted access to the PWCS network infrastructure must comply with, and are responsible for monitoring, enforcing, and reporting infractions of the PWCS Responsible Use and Internet Safety Policy.

1. Central office managers (i.e., department supervisor or director) and principals and other school-based administrators shall be responsible for ensuring that this Responsible Use and Internet Safety Policy and Regulations 923-1, "Commercial Advertising," and 295-2, "Website Development and Implementation," are followed.

2. Administrators shall also monitor teacher use and supervise correct integration of technology into instruction.

3. Web managers within schools and central office departments shall also be responsible for ensuring that this Responsible Use and Internet Safety Policy and Regulations 923-1, "Commercial Advertising," and 295-2, "Website Development and Implementation," are followed.

4. Teachers shall be responsible for guiding and monitoring student use of PWCS computer systems and network services and for providing internet safety instruction to students.

5. Students shall be responsible for adhering to the regulation and PWCS Responsible Use and Internet Safety Policy and using PWCS computer systems and network services for assignments directly related to the curriculum.

6. Parents shall be responsible for ensuring that their children adhere to the regulation and PWCS Responsible Use and Internet Safety Policy and use PWCS computer systems and network services for curriculum related assignments.

VII. Security

A. Technology Protection Measures

PWCS Information Technology Services implements and maintains industry-leading technologies to secure and provide safe internet access to students and staff. Practical technology protection measures (or "internet filters") shall be used to block or filter internet access to inappropriate information in accordance with applicable laws. Specifically, as required by the Children's Internet Protection Act [Pub. L. No. 106554 and 47 USC 254(h)], blocking shall be applied to visual depictions of material deemed obscene or harmful to minors. Subject to staff supervision and the approval of the Director of Information Technology Services or designee, technology protection measures may be disabled or, in the case of minors, minimized for bona fide research or other lawful purposes.

It shall be the responsibility of all PWCS staff to supervise and monitor usage of the computer network and access to the internet in accordance with applicable federal and state laws, guidelines and regulations of the Virginia Department of Education, and School Board policies and regulations.

B. Cyber Security

The School Board and administration recognize the importance of remaining vigilant against any and all cyber threats, while recommitting to ensuring our employees and students can use new digital tools and resources fearlessly, skillfully, and responsibly. PWCS staff are expected to take measures to decrease their susceptibility to malicious cyber activity by choosing stronger passwords, updating software, and practicing responsible online behavior. For additional resources see Appendix I.

C. Employee and Student Data Privacy

These standards are structured to provide due diligence and compliance with applicable federal, state, and local laws and School Board policies and regulations for the protection of confidential information and privacy of student and employee information during the collection, transfer, storage, use, disclosure, and destruction of such information. To protect the privacy of employees and students, school system personnel are legally responsible for safeguarding the information collected about and from employees and students. The data should be kept intact from accidents, unauthorized access, theft, unauthorized changes, or unintentional release. Data handlers should understand what is considered appropriate and inappropriate access to data and use thereof. Changes, alterations, and distribution of data must be made only in authorized and acceptable ways. No encryption solution or file-sharing program may be utilized unless authorized and approved by the Director of Information Technology Services or designee.

The collection, use, and dissemination of personally identifiable student or employee information shall be strictly limited to bona fide educational or administrative purposes. Photos and names of students and staff are allowed on PWCS websites for the purpose of publicizing school activities or student achievement, but such information must be used with caution and in accordance with Student Educational Records and Release of Directory Information Regulations 790-1 through 790-4, which gives students and their parents/guardians the right to opt out of public disclosure of their names, photos, and other student information. Information regarding individual students may only be used if it meets the definition of directory information contained in Regulation 790-3, and the student/parent/guardian has not opted out of such disclosure.

Social security numbers shall not be collected, disseminated, or disclosed, unless authorized by law. Personally Identifiable Information (PII), such as names, job titles and descriptions, telephone and fax numbers, email, and other addresses, may be collected and used internally for PWCS program/ seminar registration via the internet or for participation in PWCS online programs or other legitimate PWCS purposes. Such information shall not be sold or shared with any external groups nor disclosed to any third party outside PWCS.

Files containing confidential or sensitive data may not be stored on removable media or mobile devices taken off PWCS property unless protected by an approved Information Technology Services encryption and storage solution.

Individuals, school affiliated entities, or companies under contract with PWCS may have access to information in the course of the service they provide to PWCS, but those entities are not permitted to use or re-disclose that information for unauthorized purposes and must sign a PWCS nondisclosure agreement prior to work being performed. No other entities are authorized to collect information through PWCS sites. School affiliated entities such as an alumni association, booster club, parent teacher association, parent teacher student association, public education foundation, public education fund, or scholarship organization that provides support to PWCS, must protect student personal information.

All web- or cloud-based, PWCS hosted or vendor-hosted systems that interact with student, employee, or PWCS confidential information must provide a secure protocol for access and authentication to the system. Said systems shall provide secure FTP, HTTPS, or equivalent protocol for any necessary data transfers or interfaces between the systems, if applicable.

Risk Management and Security Services must be notified immediately if sensitive or critical PWCS information is compromised or lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of PWCS information systems has taken place, or is suspected of taking place.

D. Access to PWCS Computer Systems and Network Services

Employees, students, and temporary employees of PWCS acknowledge their understanding of the Responsible Use and Internet Safety Policy as a condition of receiving access to the computer system and network services. All employees will be reminded of the PWCS Responsible Use expectations annually in employee newsletters (i.e. “Communicator,” “The Division Leader”). Building administrators and/or department supervisors are responsible for reviewing the expectations with their staff.

E. User Accounts and Authentication

All user-level, system-level, email, and application services must have a unique user identification. Users shall not allow others access to their account and are responsible for all activities performed with their account. Additionally, employee and students must not use the accounts of others to perform activities on PWCS information resources. It is the

user's responsibility to ensure that this identification is not shared with others.

1. Use of generic and temporary network, application, and email accounts should not be deployed, unless approved by the Director of Information Technology Services or designee.

2. Employees are required to log out of computer sessions daily and prior to allowing another user access to a computer system in which they have an active session. Employees shall be responsible for any unauthorized use of a computer, network, or internet system by any person or student who accesses the same because or while the employee has failed to log out or lock the system as required.

3. Laptop users are required to first login to the PWCS network via their network login account to create a local user account on the laptop system in order to provide logging and accountability of use while off site.

4. All employees are required to take "Security Awareness Training" annually with renewal of their network login, or upon failure of simulated, or actual phishing. If after 30 days the employee has not completed training, their network access will be removed until training is completed.

5. New employees will take "Security Awareness Training" during their onboarding through the Office of Human Resources.

6. Employees who repeatedly fail simulated or actual phishing campaigns may be reported to their supervisor for personnel action.

F. Passwords

A password is used in conjunction with a unique user identification in order to authenticate a user's right to access a computer system and application service. Passwords help protect against misuse by seeking to restrict use of PWCS systems and networks to authorized users. Authorized users are responsible for the security of their passwords and accounts. Passwords are considered secret and are not to be shared under any circumstance. Individual user passwords must never be embedded into an application or process. All user-level, system-level, email, and application service passwords must conform to these standards. Public computers, such as those in a library or in labs, with no critical or sensitive information, may be excluded on a case-by-case basis, as approved by the Director of Information Technology Services or designee.

A unique password should be assigned to each user. Users are required to change passwords immediately upon first logging into the system and/or application. PWCS passwords should not be used for non-PWCS systems and services such as personal computers, banking, websites, social media, etc.

If an account or password is known or suspected to have been lost, stolen, or disclosed, the user shall immediately report the incident to the Director of Information Technology Services or designee, and change all passwords. Password requirements are located in Appendix II.

G. Electronic Communication Resources (Application Service Providers)

Employees are assigned PWCS email and messaging accounts, to be utilized for educational purposes and official PWCS Division communication.

Schools or classrooms using external electronic resources must have a teacher/administrator sponsor for each electronic resource. Accounts include but are not limited to email, blog, discussion board/forum, and social media accounts. Sponsors are responsible for guiding and monitoring student communication and use of the network. Sponsored external electronic accounts and applications are subject to the same Family Educational Rights and Privacy Act (FERPA) disclosures (e.g. parental requests, subpoena/court order requests) as PWCS maintained applications. Each school "sponsor" is expected to provide access to or export content when requested by IT or Records Center staff in response to FERPA disclosures. Any misuse of resources will cause the loss of accounts and/or disciplinary action. Sponsors will assume responsibility for teaching the students proper techniques and standards for participation and for explaining issues of privacy, copyright infringement, tool use, and network etiquette.

H. Acquisition of Hardware, Software, and Online Resources

Prior to acquiring hardware, software, and/or online resources that have not been previously approved, the Office of Information Technology Services must be contacted. Staff are required to enter a helpdesk ticket to initiate this process. If a data breach or the unintended exposure of data occurs on systems that did not utilize this approval process, the staff member(s) who provided this access will be held responsible.

The Division's malware/anti-virus software must be installed, enabled, and kept up-to-date on all network connected computer systems at all times. Computer systems must have the most recently available and appropriate software security patches commensurate with the identified level of accepted risk.

Computers and monitors should be turned off to conserve energy when not in use. On occasion, staff may be directed to leave computers on for software updates and other reasons that are communicated by the division.

I. Remote Access

PWCS employees, contractors, vendors, who access PWCS resources remotely via VPN (Virtual Private Network) must adhere to this Responsible Use Policy. Organizations or individuals who wish to implement non-standard remote access solutions to the PWCS network must obtain prior approval from the Director of Information Technology Services or designee. All computer systems that are connected to the PWCS internal network via remote access technologies must comply with all requirements of this regulation.

VIII. Incident Response, Mitigation, Management, and Investigation

All identified security related incidences shall be reported to a site administrator or Risk Management and Security Services immediately. The office of Risk Management and Security Services or the Director of Information Technology Services or designee shall determine what, if any, action needs to be taken. No user shall power off/on, disconnect, delete information from, or otherwise disturb any computer subject to seizure, unless under the direction of Risk Management and Security Services or the Director of Information Technology Services or designee.

IX. Preservation of Electronic Evidence

When the Division has notice of actual or anticipated litigation, it is required to preserve all evidence, including electronic evidence, related to such litigation. Employees who receive notice from PWCS of actual or threatened litigation (or become aware of such actual or threatened litigation from other sources) must preserve all such evidence and may not delete, alter, or otherwise disturb the integrity of any electronic evidence. This includes, but is not limited to, emails, files, folders, or any other electronic data or communications.

X. Internet Safety Instruction

Internet safety instruction is the responsibility of all instructional personnel and resources can be found on the PWCS web sites.

The Associate Superintendent for Communications and Technology Services (or designee) is responsible for implementing and monitoring this regulation.

This regulation and related policy shall be reviewed at least every five years and revised as needed.

APPENDIX I - Resources

Contacts for Security Incidents

1. Site administrator, principal, school counselor, or department supervisor
2. Risk Management and Security Services 703.791.7206
3. Information Technology Services 703.791.8722
4. PWCS "Code of Behavior" on the PWCS website (pwcs.edu)
5. Regulation 503.02-1 "Standards of Professional Conduct"

Cyber Security Resources

1. www.DHS.gov/StopThinkConnect to learn more about cyber security

APPENDIX II - Password Requirements

PWCS-Managed Accounts. Password requirements for PWCS managed accounts will be enforced as appropriate for use and risk involved. PWCS intentionally isn't sharing these details in this public document to allow for flexibility in these dynamic requirements as well as to better secure our systems.

Non-PWCS-Managed Accounts. Staff and students who utilize non-PWCS-managed accounts should utilize either the Complex Passwords or Passphrase requirements below. Either are acceptable to use and the system requirements may dictate which is acceptable by the vendor system. Two-factor authentication is strongly encouraged – especially if there is sensitive data and/or financial implications.

Complex Passwords. Passwords for non-PWCS managed accounts must meet the minimum requirements below:

1. 8 characters or more
2. Passwords must contain numbers and letters
3. Contain upper and lower case letters
4. Contain special characters, such as, !@#$%^ `&*()
5. Do not include First Name, Last Name or Login ID
6. Changed Frequently (3 months)
7. Examples: T3@ch!nG*, StR*nG43x

Passphrases. Passphrases for non-PWCS managed accounts must meet the minimum requirements below:

1. Minimum 24 characters, but can/should be longer
2. It is not essential to use numbers, special characters, or change the passphrase frequently (can use this for years)
3. Examples: EverymorningIliketodrinkStrongcoffee, StarsandtheM00nandapeanutbutterspoon