Security Practices – ELMS Users

The Early Learning Management System (ELMS) is a Secure, Web-Based Data System

ELMS is an internet site, protected by firewalls and anti-virus scanning of all DCYF servers.

ELMS Enforces the Following Password Criteria

- At least 8 characters
- At least 1 or more of the following:
    - Lower-case letter
    - Upper-case letter
    - Number
    - Special character

Best Practices When Accessing Web-Based Data

All Staff Accessing ELMS Should Practice the Following

- Do not send confidential data via wireless technology, email or the internet unless the connection is secure, or the information is encrypted.
- Do not store unencrypted confidential information on mobile devices, laptop/desktop computer hard drive, USB drive, CD, flash memory card or other storage media.
- Do not share ELMS login credentials.
    - Each ELMS user should have their own unique username and password.
- Do not write passwords down or save passwords on your computer.
- Do not use public WiFi networks to access ELMS.
- Avoid unsecured websites, especially when accessing ELMS.
- Always lock your computer before leaving it unattended.
- Use a strong password to access ELMS.
    - 12 or more characters is best.

Questions?

For all ELMS technical and access questions, email ELMS support at **ELMS@dcyf.wa.gov**.