LWV LEAGUE OF WOMEN VOTERS®
OF RIDGEWOOD

DATA SECURITY TIPS FOR PARENTS

The pandemic has increased our reliance on online services, not only for school and work but also for doctor’s visits and banking. To help stay web-safe, here are tips for parents and anyone else interested in maintaining data privacy and security.

To prevent data hacks:

- Secure your home WiFi router, network, and modem (i.e., purchase a WiFi router with built-in security, use a VPN on personal devices, purchase internet security, ask your cable provider about enhanced security features/services, check out tutorials online to secure your home network).
- Protect personally identifiable information (name, address, social security number or other identifying number or code, telephone number, email address) whenever possible.
- Conduct financial transactions on websites that secure or encrypt data (check the address bar for a padlock icon) and over secure internet connections (uses “https” in the URL).
- Avoid saving your family's personally identifiable information on a network computer or device.
- Choose strong passwords of nine characters or more, and do not share them or write them down where others can easily discover them. Do not use the same password across multiple sites. You can use an online password generator and save them into a password manager.
- Adhere to the school district's Acceptable Use Policy and remind children not to share their passwords with anyone.
- Limit sharing of your phone/email contacts when prompted by third-party apps.

To limit what data is being shared:

- Choose a web browser that has strong privacy and security settings on personal devices (e.g., Google, Firefox, Safari, etc.) and customize as you see fit.
- Choose a search engine on personal devices that protects your privacy and avoids/limits using algorithms to determine personalized search results (e.g., DuckDuckGo).
- Consider using family privacy control settings on personal devices, whenever possible.
- Carefully read and acknowledge the district’s Acceptable Use Policy agreement form regarding student data and privacy for all students in your family. If your children are old enough to submit the forms themselves, discuss privacy issues with them in advance.
- Learn more about how your children’s data is being collected and used at school and home, etc. This includes social media accounts and all apps (educational, sports teams, games, health/medical, financial), plus smart devices, wearables, and WiFi-enabled accessories.
- Choose apps, hardware, and software that are ranked safe by the FBI, FTC, and consumer advocacy groups.

- Check the age appropriateness of your children’s video games and preferred online content. Common Sense Media is one site that evaluates children’s games and apps.
- Teach your children to limit what they share online, including photos, videos, and voice recordings. Discourage children from posting images of themselves online, including identifiable information such as their room, house, car, or personal effects.
- Determine web safety rules for your family that are practical. If cameras cannot be turned off during online meetings, use a background blur or virtual background.
- Teach your children to be careful of the friends they make online. Both the FTC and the FBI post online safety information on their websites.
- Monitor your children’s phone, tablet, and gaming regularly. Keep communication lines open with children, and let them know you are there to support them when they have concerns.

To prevent data loss:

- Regularly backup important data to external physical drives, not only to the Cloud.

Select resources:

- Common Sense Media
    - https://www.commonsensemedia.org/
- FTC on pandemic privacy
    - https://www.ftc.gov/news-events/blogs/business-blog/2020/06/privacy-during-coronavirus
- FTC on facial recognition risks
    - https://www.ftc.gov/news-events/blogs/business-blog/2021/01/facing-facts-about-facial-recognition