Security for Internet Access at UGDSB

The Upper Grand has significantly enhanced its ability to monitor and protect our network and users. While supervision is always important we recognize that schools require greater support. In the last year the IT Dept. has invested in a number of services and strategies to protect the integrity of our network and the safety of our students and staff.

Malware and Virus

- ESET NOD32 - antivirus and antispyware on all laptops, desktops, and servers
- Barracuda - email - antispam and phishing software deployed at the Board Office

Inappropriate content

Web Filtering (categories and exceptions)

- VPN blocking (no VPN's allowed)
- DNS Safe Search (Search on Google only brings back appropriate information)
- SysCloud - monitors for inappropriate language inside Google Docs
- GMail restrictions
    - No outbound or inbound mail
    - Objectionable content filters

Social Media Restrictions

- YouTube restrictions
    - Elementary
        - students can only see "appropriate" content as determined by Google
    - Secondary
        - Students must sign in to Youtube to have access
- Facebook and Twitter allowed
- Spotify, Snapchat, Instagram blocked