User Accounts and Passwords Regulation

3350-10 | User Accounts and Passwords Regulation

Date Approved: February 14 2012
Date Amended: October 06 2017

Access to district technology or networks is normally provided to all students and employees of the district. Access is provided subject to the terms of the Acceptable Use of Technology Policy and its accompanying regulations. In order for students to receive access, their parents or guardians and the student must sign a district user agreement acknowledging their understanding of the district policy and regulations. Principals must verify that students are not granted access to School District Technology until they and their Parents sign the district user agreement and must maintain completed user agreements for all students at the school.

Access to district technology or networks is a privilege and not a right. Unacceptable, inappropriate or illegal use of resources on the Internet, email or other online actions that violate the district Code of Conduct, school Code of Conduct or the Acceptable Use of Technology Policy or Regulations, may result in a removal of access privileges. The district may deny, revoke, suspend or remove any user account or access at any time based upon a reasonable determination of unacceptable use by the user. The final decision as to whether unacceptable behaviour has occurred resides with the Superintendent or designate.

Passwords

- The district has a formal password requirements detailed in the Microsoft Active Directory Group Policy which applies to the majority of systems. There are additional password policies for systems which are not secured by Microsoft Active Directory. Those password policies will be communicated to all users that require access to those systems.
- Users are responsible for safeguarding their passwords for access to district technology and networks. Individual passwords are not to be printed, hand written, stored on-line or shared with others unless the Superintendent or designate grants an exception.
- Users are directly responsible for all actions and transactions that are made using their individual username and password combination. No user may access district technology or networks with another user's credentials with the exception of the Information Technology Department for troubleshooting purposes or with permission granted in writing by the Superintendent or designate.
- The district will never use email to ask for passwords or personal user information for district systems that you access. Any email asking for credential information should be immediately brought to the attention of a teacher, principal or supervisor and the Manager of Information Technology

Email

- District email accounts are provided for the purposes of exchanging information consistent with the Acceptable Use of Technology Policy and Regulations.
- All employees are expected to access and use their district email accounts on a frequent and regular basis.
- Email use in the district is subject to all district policy, regulation and practice.
- Personal use of a user's district email account is permitted as long as the Acceptable Use of Technology

Policy and Regulations are followed

Storage of Files

- Users are provided with a folder (the “H” drive) for the purposes of storing information consistent with the Acceptable Use of Technology Policy and Regulations.
- The district has implemented disaster recovery plans for the email system and for data stored on the “H” drive. It is the user’s responsibility to ensure their personal work is stored on the “H” drive so that it will be backed up.
- When a user leaves the district, their accounts (both email and storage) will be immediately disabled, but not deleted for a minimum of 30 days. Final deletion of user accounts is at the discretion of the Secretary-Treasurer or the Superintendent. A disabled account of a user that has left the district may be re-activated and the password reset at the direction of the Secretary-Treasurer or the Superintendent.

Expectation of Privacy

Users should understand that all use of district technology or networks is subject to monitoring and review by the district. Further information on this is provided in Regulation 3350-40 Data Security and Privacy.

School District Property

- All files and data generated under the employ of the district, or while a student of the district, are the property of the district.
- District property may be used only for legitimate educational or operational purposes, or for other purposes referred to in the Acceptable Use of Technology Policy or Regulations.

Related Policies and Regulations:

Bylaw #7	Freedom of Information/Protection of Privacy Bylaw
1410	District Code of Conduct Policy
3350	Acceptable Use of Technology Policy
3350-20	Acceptable Use of District Technology Regulation
3350-22	Prohibited Use of District Technology Regulation
3350-25	Bring Your Own Device Regulation
3350-30	Technology and Instruction Regulation

3350-40	Data Security and Privacy Regulation
3350-50	District and School Websites Regulation
6710	Records Management Program Policy