| | Lloydminster Catholic School Division – Administrative Procedures |
|---|---|
| | **AP 145 – Network System Services:  MAN/Internet Access** |
| Related LCSD AP's | AP 144 – Information Security<br>AP 180 – Freedom of Information and Protection of Privacy<br>AP 306 – Technology / Online Acceptable Use (Student)<br>AP 481 – Employee Acceptable Use of Technology |
| Form(s) | |
| References: | *The Education Act, 1995* sections 85, 87, 175 |
| Received by the Board:<br>April, 2025 | Update:<br>April, 2025 |

**Background**

The Division deploys a Metropolitan Wide-Area Network (MAN) in conjunction with Alberta SuperNet for access to the Internet.  This network allows staff and students to access online resources along with the means to communicate with each other and throughout the world. In addition, this network will provide staff and students with access to a multitude of administrative and instructional resources from both local and cloud repositories of digitally stored information.

The Division will provide Internet services, students can use to access instructional and reference material on the Internet. These services are designed and supervised so that objectionable materials are not readily available. Students and parents must be informed that inappropriate materials may be encountered inadvertently by students during the course of their research. However, if inappropriate material is accessed, the student shall disengage immediately. Students are taught the skills necessary to evaluate information and resources as part of their ongoing education for life in a world with instant access to voluminous information.

**Procedures**

1.  Guiding Principles

    1.1     The Division may provide employees and students with access to the Division's network system services, which includes: email (Microsoft 365), Google Workplace for Education, Intranet data, and Internet applications and resources.

    1.2     The Division's network services have been designed to provide students and staff with access to a wide range of information and the ability to communicate with people throughout the world. The division's network system services will also be used to increase internal professional collaboration and communication.

    1.3     Users may not use the Division's system for commercial purposes, (defined as offering or providing goods or services) except for authorized Lloydminster Catholic School Division services (e.g. student fee payment, etc.)

1.4 The term "educational purpose" includes use of the system for classroom activities, professional or career development, and independent study activities.

2. Responsibilities of Division Personnel

    2.1 The IT Manager shall:

        2.1.1 In consultation with Network System Supervisor, be responsible for the network system plan, security, maintenance, and performance monitoring.

        2.1.2 Work collaboratively with both Alberta and Saskatchewan government ministries along with technology sector businesses and agencies as required for both regulation compliance and operational reliability.

        2.1.3 Allocate network system usernames and passwords for all students.

            2.1.3.1 LCSD email (Google)

            2.1.3.2 Google Docs

        2.1.4 Along with school administration, hold student usernames and passwords in strict confidence.

        2.1.5 Permit Library Technicians the ability to reset student Google workspace account passwords.

    2.2 The Principal will serve as the building-level coordinator for the system, approving building-level activities (for example; social media page for a fundraising event, etc.), ensuring teachers receive proper training in the use of the system, establishing a system to ensure the onsite supervision of students using the network system, maintaining user agreements, enforcing the Division's acceptable use protocols (Administrative Procedure 306 Technology/Online Acceptable Use (Student) and AP481 Employee Acceptable Use of Technology) at the building level.

    2.3 The IT Department will establish a process to:

        2.3.1 Create individual / class accounts;

        2.3.2 Monitor and administer network account retention procedures for both students, staff, and guests;

        2.3.3 Establish and monitor a virus protection process;

        2.3.4 Establish and monitor system backup procedures; and

        2.3.5 Initiate other activities deemed necessary at the school or division level.

3. Access to the System

    3.1 Acceptable Use Protocol

        The Division's acceptable use protocols (AP306 Technology/Online Acceptable Use (Student) and AP481 Employee Acceptable Use of Technology) will govern all use of the Division's network system services. Student use of the system will also be governed by the Division's supervision and discipline administrative procedures.

3.2 Internet Access

3.2.1 All Division employees and students will have access to the internet on Division devices through the Division's network system services.

3.2.2 All students, staff, and guests will have access to the internet using their PED through the Division's "Guest" wireless network.

3.3 Individual Email Accounts for Students

All students K-12 will be provided with an individual Google Workspace for Education email account upon registration.

3.4 Individual Student Network System Services Account

All students Grades 8 through 12 shall be provided an active directory account enabling them access to the internet and other network services.

3.5 Individual System and Microsoft 365 Accounts for Division Employees

3.5.1 Division employees will be provided with an individual network system services account for use on Division devices. The IT Manager will allocate usernames and passwords. Users may change their passwords without official notification. Division employees should change their network system services account password every 120 days.

3.5.2 Division employees will be provided with a "Google for Workspace for Education" account for access to Google Workspace for Education.

3.6 Substitute Teachers:

3.6.1 All Division approved substitute teachers will be provided with a Network System Services account and Google Workspace for Education account for the duration of their approved substitute teacher status with the Division.

3.6.2 All Division approved substitute teachers will be provided with MySchoolSask access credentials when the duration of the assignment exceeds three days.

3.6.3 The designated school administrative assistant will notify the Student Records Coordinator by email regarding a substitute teacher's assignment for authorized access as per AP144 – Information Security.

3.6.4 The absent teacher may share their instructional documents or media with a substitute teacher via the substitute teacher's Google Workspace for Education account.

3.7 Guest Accounts

Guests have access to internet via access through LCSD's "Guest" account.

4. Parental Notification and Responsibility

4.1 The school will notify the parents regarding the Division's network policies governing its use and require both the parent and student to both sign the Network - Parent Permission and User Agreement Form as part of their Registration Package.

4.2 Parents shall have the right to investigate the contents of their child(ren)'s Google email files in consultation with the teacher. Parents have the right to request the termination of their child(ren)'s individual account at any time.

4.3 The Division's Acceptable Use Protocol (AP306 Technology / Online Acceptable Use (Student)) contains restrictions regarding access to inappropriate material. There is a wide range of material available on the Internet that may not be consistent with the values of our families, school, or Catholic Faith. Therefore, appropriate use of the Internet shall be governed by the intent of Board Policy 1: Division Foundation Statements that outline the Division's Mission Statement and Value Statements.

5. Limitation of Liability

5.1 The Division makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the Division system will be error-free or without defect. The Division will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. The Division is not responsible for the accuracy or quality of the information obtained through or stored on the system. The Division will not be responsible for financial obligations arising through the unauthorized use of the system.

6. Due Process

6.1 The Division will cooperate fully with law enforcement officials in any investigation concerning to or relating to any illegal activities conducted through the Division's Network System Services.

6.2 In the event there is an allegation that a student has violated the Division's Acceptable Use Protocol, the student shall be provided with a written notice of the alleged violation and an opportunity to be heard in the manner set forth in the school's discipline procedure.

6.3 Student disciplinary actions shall be directly related to the violation and shall encourage the self-discipline necessary to appropriately utilize the Division's Network System Services. If the alleged violation also involves a violation of other provisions of school procedures or Division Administrative Procedure, the violation will be handled in accordance with the applicable provision of that procedure.

6.4 Employee violations of the Acceptable Use Protocols (AP481 Employee Acceptable Use of Technology) shall be handled in accordance with Division procedures and/or the Code of Ethics governing the conduct of professional and support staff.

6.5 Account privileges of a guest user may be terminated at the discretion of the IT Manager, in consultation with the Director, or designate. The user will be given appropriate notice unless extenuating circumstances negate the need for such notice. Guest accounts inactive for more than thirty (30) days may be removed, along with the user's files without notice to the user.

7. Confidentiality of Student and Staff Information

   7.1 System users shall have a limited expectation of privacy regarding the contents of their personal files on the Division's network system services.

   7.2 Routine maintenance and monitoring of the system may lead to discovery that the user has or is violating the Division's Acceptable Use Protocols (AP306 Technology/Online Acceptable Use (Students) and AP481 Employee Acceptable Use of Technology), or the law.

   7.3 An individual search shall be conducted if there is reasonable suspicion that a user has violated the law or the school's procedures. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation.

   7.4 Division employees shall be aware that the system configuration and the security of user passwords limit the confidentiality of their personal files.

8. Instruction and Student Usage

   8.1 Division and school procedures regarding copyright infringement will govern the use of material accessed through the Division's system.

      8.1.1 Employees will make a standard practice of requesting permission, from the holder of the work, if their use of the material has the potential of being considered an infringement because the extent of copyright protection of certain works found on the Internet is frequently unclear.

      8.1.2 Teachers will instruct students to respect copyright and to request permission when appropriate.

   8.2 Division and school procedures regarding plagiarism will govern use of material accessed through the system. Students will be taught appropriate research and citation practices.

   8.3 When using Internet resources or media for class activities, teachers will select material that is age appropriate and that is relevant to the course objectives as defined by Saskatchewan Ministry Education's curriculum. Teachers will preview all internet materials, media, resources, and sites they share or recommend to students to determine the appropriateness of information to be accessed by their students.

9. Web Sites

   9.1 Division Web Site / Social Networking / Social Media

   The Division may establish a web site and may develop web pages presenting information about the Division. The Division Communications Coordinator and the Executive Administrator are responsible for maintaining the Division web site and utilization of social networks and social media.

   9.2 School or Class Web Pages / Social Networking / Social Media

   Classes may establish a web page that presents information about the school or class activities. The Principal will authorize a staff member to be responsible for the development,

screening, maintenance, and management of the class web site. Teachers will be responsible for maintaining their class site.

9.3    Student Web Pages / Social Networking / Social Media

With the approval of the Principal for an educational program enhancement, students may establish personal web pages; or personally post their educational work on a social network or social networking sites. The Principal will establish a process and criteria for the establishment and posting of material, including links to other sites, on their webpage or on a social network or social networking sites. These types of digital learning must be related to the student's educational program and career preparation activities. The Principal will authorize a staff member to be responsible for monitoring and screening the student's learning engagement on these types of digital learning.

9.4    Extracurricular Organization Web Pages / Social Networking / Social Media
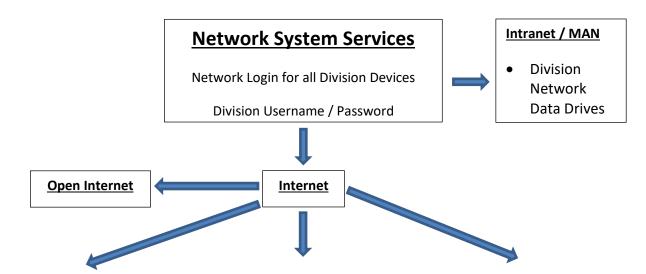
With the approval of the Principal, extracurricular organizations may establish web pages, or engage on social networking / social media sites. The Principal will establish a process and criteria for the establishment and posting of material. The Principal will authorize a staff member to be responsible for monitoring and screening the extracurricular organization's engagement on these types of digital media.

9.5    Publication of Pictures

9.5.1    Division and school web sites shall protect the identity of the student by ensuring no student in the picture is identifiable without written consent as per AP180 *Local Authority Freedom of Information and Protection of Privacy*. The names of students shall not accompany the picture.

9.5.2    The Division may publish the photograph of an employee on Division digital media or on Division documents unless the employee specifically instructs the Division not to do so.

# Lloydminster Catholic School Division

# Information Technology Access Chart

**1. Access to Division Network System Services by Full Time Employees:**

**Network System Services**

Network Login for all Division Devices

Division Username / Password

➡️ **Intranet / MAN**

- Division Network Data Drives

⬇️

**Open Internet** ⬅️ **Internet**

**Student Information System Applications**

- Single Sign On
- Authorized users will be provided access to the following services according to employee role and responsibilities:
  - Student Data System
  - PASI
  - Destiny
  - School Messenger
  - Bus Planner

**Financial Systems and Records (Atrieve)**

- NSS Username & Password Login will provide "Read Only" access.
- A distinct username and password are required for access to "write" capability for each financial application.

**Google Workspace for Education**

- Google
- Microsoft 365
- Amazon
- BMO
- School Cash Online

2. **Contracted Employee Access to Division Network System Services:**
   Authorized contracted employees will be provided access to the following network system services:

   a. **Teachers**
      i. The IT Manager will provide a distinct username/password (annual) to the employee for access to:
         1. Network System Services
         2. Google Workspace for Education username/password (annual)
      ii. Services:
         1. Division email (Microsoft 365) services (annual)
         2. MySchoolSask – The Student Records Coordinator will authorize access for the period of assignment.

   b. **Educational Assistants**
      i. The IT Manager will provide a distinct username/password (annual) to the employee for access to:
         1. Network System Services
         2. Google Workspace for Education username/password (annual)
      ii. Services:
         1. Division email (Microsoft 365) services (annual)

   c. **Administrative Assistant**
      i. The IT Manager will provide a distinct username/password (annual) to the employee for access to:
         1. Network System Services
         2. Google Workspace for Education username/password (annual)
      ii. Services:
         1. Division email (Microsoft 365) services (annual)
         2. School Office Network Drives
         3. MySchoolSask – The Student Records Coordinator will authorize access
         4. Bus Planner – The Transportation Supervisor will authorize access

   d. **Library Technicians**
      i. The IT Manager will provide a distinct username/password (annual) to the employee for access to:
         1. Network System Services
         2. Google Workspace for Education username/password (annual)
      ii. Services:
         1. Division email (Microsoft 365) services (annual)
         2. Follett Destiny – The Learning Resources Coordinator will authorize the Library Technician's access to Follett with a distinct username/password (annual).

  e. **Bus Driver**
    i. The IT Manager will provide a distinct username/password (annual)
     to the employee for access to:
      1. Network System Services
    ii. Services:
      1. Division email (Microsoft 365) services (annual)

3. **Substitute Employee Access to Division Network System Services:**
  Short-term employees who are authorized by administration to act as a substitute employee will be
  provided access to the following network system services:
    a. **Teachers**
      i. The IT Manager will provide a distinct username/password (annual)
       to the employee for access to:
        1. Network System Services
        2. Google Workspace for Education username/password (annual)
      ii. Services:
        1. Division email (Microsoft 365) services (annual)
        2. MySchoolSask – The Student Records Coordinator will authorize access
         for the period of assignment in excess of three (3) days.

    b. **Educational Assistants**
      i. The IT Manager will provide a distinct username/password (annual)
       to the employee for access to:
        1. Network System Services
        2. Google Workspace for Education username/password (annual)
      ii. Services:
        1. Division email (Microsoft 365) services (annual)

    c. **Administrative Assistant**
      i. The IT Manager will provide a distinct username/password (annual)
       to the employee for access to:
        1. Network System Services
        2. Google Workspace for Education username/password (annual)
      ii. Services:
        1. Division email (Microsoft 365) services (annual)
        2. MySchoolSask – The Student Records Coordinator will authorize access

    d. **Library Technicians**
      i. The IT Manager will provide a distinct username/password (annual)
       to the employee for access to:
        1. Network System Services
        2. Google Workspace for Education username/password (annual)
      ii. Services:
        1. Division email (Microsoft 365) services (annual)
        2. Follett Destiny – The Learning Resources Coordinator will authorize
         access to Destiny

    **e. Bus Driver**
          i. The IT Manager will provide a distinct username/password (annual) to the employee for access to:
              1. Network System Services
          ii. Services:
              1. Division email (Microsoft 365) services (annual)
              2. Bus Planner: The Transportation Supervisor will authorize access to Bus Planner