Aurora Academic Charter School Administrative Regulation

Category: **G. Curriculum and Instruction**

Code: AR 7040.1

Policy Name: **Staff Technology Policy**

Issue Date	**August 10, 2020**
Revision Date	
Review Year	**2023**

Objective:
To support the implementation of BP 7040 Technology Policy.

Aurora School supports and encourages responsible use of technology. Our goal is to ensure that data integrity and security meets and/or exceeds legislative requirements.

This administrative regulation applies to staff use of technology in any school-related activities or school-related data . In cases where irresponsible or unethical use is detected, disciplinary measures may be considered.

Responsibility:
Managed by the Superintendent, Secretary Treasurer, and supervised by the Systems Administrator.

Regulation:

1. Technology will be accessible to individual employees based on employment profile.
2. All staff must sign a technology declaration (Appendix A).
3. Passwords must be kept confidential and login credentials must not be saved to their respective program, site, data base, or application.
4. The Superintendent and Secretary Treasurer reserve the right to change technology controls to ensure best data security practices.
5. Data must be stored on the school network or secured school drives. Information stored on a portable storage device must receive prior approval by the staff's direct supervisor and be password protected or encrypted.
6. Aurora will make the best attempt to ensure staff have the required technology to operate within their roles. In the event a staff member is required to use personal technology for employment purposes, please refer to "Aurora Staff Guidelines when working from home" (Appendix B).
7. In the event of a privacy breach or suspected privacy breach, the Superintendent, Secretary Treasurer and Systems Administrator must immediately be notified.

References:
BP 2040 Member Code of Conduct
BP 7040 Technology Policy
The Education Act / PASI Agreement

APPENDIX A

Staff Technology Declaration

Staff are responsible for appropriate behaviour when using technology.

Staff Declaration

Respect and Protect Myself

- Will be the sole user of my school account(s) and protect my passwords by not sharing them with others or by saving login credentials for auto-login. .
- Will follow school procedures and professional standards.
- Will take responsibility to ensure I understand and comply with legislative requirements/enforcements regarding use of technology.

Respect and Protect Others

- Will take due care when sending, receiving, entering and updating sensitive school/student information.
- Will be sure to protect school technology and data.

Respect and Protect Intellectual Property

- Will follow federal copyright laws and fair use guidelines.
- Will respect and protect information owned by Aurora School Ltd.

Respect and Protect Aurora School Property and Equipment

- Will take full responsibility for, and respectfully use, any technology available to me at all times.
- Will use network bandwidth, file storage space and printers reasonably and responsibly.
- Will report abuse of technology to a school administrator and/or designate.
- Will report security or network problems to a school administrator and/or designate.

I, _____, have read, understand, and agree to the above conditions.

Staff Signature: _____ Date: _____

Supervisor Declaration

I have carefully reviewed this document with **_____** and agree to the above conditions.

Print Supervisor Name: _____

Signature: _____ Date: _____

APPENDIX B

AURORA STAFF WORKING FROM HOME

Aurora Staff Guidelines when working from home

All professional standards and security of data continue whether working from school or at home at any time.

Home is defined as your current residence in or near the community of work.

Working from Home

In situations when Alberta Health Services/Alberta Education has mandated school site closures, teachers and support staff who request to work from home may do so by applying to their principal or immediate supervisor. Each school should develop a check-in procedure for staff.

If the work requires the employee to be at school, administrators will work with them to identify risk mitigation measures to enhance their safety and increase social distancing measures as directed by the most current advice from the Alberta Chief Medical Officer and Alberta Education:

- The role requires the employee be physically present (e.g. custodian, admin assistant, administrator);
- The role requires the employee to access information or systems that are not available in the home environment;
- The role involves sensitive or confidential information or records that cannot, and should not, be transferred from/to the home environment.

Working from Home Guideline

To work from home the employee must have the ability to complete assigned deliverables and day-to-day functions (plan, assess, and professional development), as well as to communicate with colleagues, administration, students, and parents in a secure environment.

The principal or immediate supervisor may call you back to your work site, based on operational needs.

Regardless of where you are working, the following are important expectations to remember:

- Employee and student safety is our primary concern. Please maintain a safe and secure work environment. Aurora School is following the directives from Alberta Health Services and Alberta Education to ensure we are complying with Occupational Health and Safety regulations.
- Continue to follow all Division policies and administrative procedures.
- The Division will be setting expectations for work hours and employees must be available and accessible during the workday.Periodic attendance at your workplace may be required. This may include a directive to return to the normal work site on short notice during normal work hours.
- Check-in daily, or on an agreed upon schedule, with your administration for support and/or a progress update.

- attend scheduled meetings via conference calls or web-based meetings.
- Leave entitlements follow the usual process for requests and approvals. These include personal, sick, family needs, compassionate and all other leaves identified in collective agreements. Requests for leave should be accessed in the same manner in which you typically request them. Continue to follow regular procedures for applying for/notifying HR about medical and other absences. When working from home it is expected that you comply with professional and legislated professional standards.
  - maintain privacy: cannot be overheard by family, no family members/home visitors wandering into meeting
  - maintain security of technology and data at all times
  - professional dress
  - ensure appropriate computer screen and live video backgrounds & close all web windows except ones being used for Lesson

Equipment and Technology

- Division Laptop\Chromebook\IPad may be signed out by your administrator to work from home.
- You are responsible for ensuring your working from home environment has appropriate telephone/internet connectivity and security. If you cannot work from home, you can speak to your supervisor regarding a safe and secure work environment at school.

IT Security and Privacy guidelines

- The use of personal email for work purposes is strictly prohibited. All secure data and information must be kept on Divisional drives.
- Staff should use divisional cloud-based approved and secured platforms (OneDrive/ Google Drive). Contact your administrator and/or Aurora IT administrator for additional support.
- Adequate safeguards must be put in place to avoid data and privacy breaches. If you require support, contact the IT Help Desk .
- If you suspect a privacy breach, please call your administrator for these matters immediately.
  Important note: Protect yourself and the Division from malicious attacks by:
  - Never open attachments or links in emails that are suspicious.
  - Beware of any email asking for urgent action. If it's that urgent, they will contact you again.
  - Do not reply to the email if unsure.
  - Check to whom the email is addressed. Remember, phishing emails are rarely specific.
  - Watch for spelling and grammatical mistakes. Often, these can be a tell-tale sign of phishing.
  - Hover over the link in the email without clicking on it. Will the displayed link take you to where you would expect?
    - Does the signature look genuine?
  - **Report the email by calling System Administrator**
    - **Do not forward the email. Doing so may exacerbate the problems the phishing email can cause.**
  - For Google based email systems, click on the three vertical dots in the upper right-hand corner of an email received from outside the local network. Options to either ‘Report spam’ or ‘Report phishing’ are available.

- It is suggested that emails believed to be phishing or spam should simply be deleted by the person receiving it, and that person can just send the Aurora System Administrator a new email indicating a suspected phishing email was received from “type out the Sender email.” For any additional questions, please contact your administration.