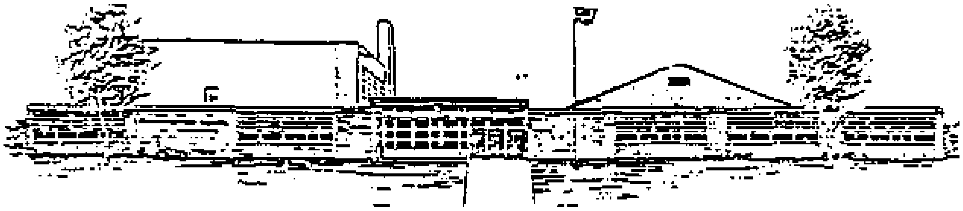
**STARKWEATHER SCHOOL DISTRICT #44**

***Sarah Beck-Connot***
*Superintendent &*
*Secondary Principal*

***Alysson Groves***
*Elementary Principal*

***Julie Wass***
*Business Manager*



*505 E Main Street*
*P.O. Box 45*
*Starkweather, ND*
*58377-0045*

*Phone: 701-292-4381*
*Fax: 701-292-5714*

## Computer Science & Cybersecurity Integration Plan

### Introduction and Purpose of the Plan

In compliance with HB 1398 and recognizing the critical importance of computer science and cybersecurity education, Starkweather Public School District is committed to integrating robust programs into our curriculum. Despite being a small rural district, we believe access to quality education in computer science and cybersecurity is essential for preparing students for the digital age.

The integration plan outlines how Starkweather Public School District intends to comply with North Dakota's new state mandates per HB 1398. The district's focus will be awareness for grades K-5, exploration for grades 6-8, and preparation for grades 9-12.

### Goals and Objectives

1. Curriculum Development – develop and implement a comprehensive computer science curriculum tailored to the needs and capabilities of our students, starting in elementary up to high school grade levels.

2. Educator Training and Awareness – provide educators cybersecurity awareness training to enhance their understanding of online safety, privacy protection, and cybersecurity best practices. Offer professional development opportunities for all educators to improve their proficiency in teaching computer science and integrating cybersecurity concepts across various subjects. Provide resources to the library media specialist and business educator to earn a Level 3 endorsement to comply with HB 1398.

3. Infrastructure & District Enhancement – upgrade technology infrastructure to support the implementation of computer science and cybersecurity programs, including the provision of necessary hardware, software, and internet access.

4. Community Engagement – foster partnerships with local businesses, community organizations, and cybersecurity professionals to enrich the learning experience and provide real-world exposure to computer science and cybersecurity concepts and careers.

**Implementation Plan**

1. Curriculum Development

- Collaborate with educators to design a standards-aligned computer science curriculum to integrate computational thinking, coding, and digital literacy skills.
- Ensure the curriculum is adaptable to accommodate the varying proficiency levels of students and incorporates hands-on learning opportunities.

2. Educator Training and Awareness

- Organize workshops and seminars on cybersecurity topics relevant to students, such as online safety, password management, and social media awareness.
- Implement age-appropriate cybersecurity education materials and resources to engage students in understanding cybersecurity risks and promoting responsible online behavior.
- Facilitate professional development workshops and training sessions for educators to enhance their knowledge and teaching skills in computer science and cybersecurity.
- Provide access to online courses, certifications, and resources to support continuous learning and skill development among educators.

3. Infrastructure Enhancement

- Assess the current technology infrastructure and identify areas for improvement, such as upgrading hardware, software, and network security measures.
- Seek funding opportunities and grants to support infrastructure enhancements and ensure equitable access to technology resources for all students and educators.

4. Community Engagement

- Establish partnerships with local businesses, cybersecurity firms, and industry professionals to offer mentorship programs, internships, and career exploration opportunities for students.
- Organize events such as hackathons, coding competitions, and cybersecurity awareness campaigns, to showcase student achievements and promote community involvement in computer science education.

**Teacher Credential Information**

Starkweather Public School employs one business educator for grades K-12 who holds a Level 2 credential. If or when the district hires a new business teacher, the district will require the individual have or be able to acquire a Level 2 credential as approved through the Education Standards and Practices Board (ESPB). The district will also provide incentives to pursue a Level 1 credential, including but not limited to, tuition reimbursement or assistance.

Starkweather elementary teachers will all earn a Level 3 credential via professional development during August 2024 in service dates. Code.org, Center for Distance Education, Regional Career and Technical Centers, Microsoft TEALS Program, etc. may be used to train elementary teachers via completing credits and/or micro-credentials.

**Existing Capacity and Implementation Needs**

At the elementary level, educators will introduce cybersecurity and programming concepts to students grades K-5. Teaching concepts to kindergarten students will be approached in a simplified and age-appropriate manner. As students move through the grade levels, concepts will become more involved. Elementary educators recommend integrating these concepts and new standards as elementary students may benefit from small doses of cybersecurity and programming concepts in varied topics. Elementary educators will collaborate with the high school business teacher for guidance and ensuring standards are woven in with current curriculum.

At the middle school level, the business education instructor will explore concepts by integrating cybersecurity and programming curriculum within lessons and make use of cross-curricular projects. The seventh and eighth grade keyboarding and personal finance course assignments may focus on introductory concepts. Seventh and eighth grade stand-alone exploration courses may be offered if/when schedules would allow it. STEM courses is also available for seventh and eighth grades as well as high school grades nine through twelve.

Grades nine through twelve will have stand-alone cybersecurity and programming courses to prepare them for the digital world they will enter after high school. Master high school schedules will include classes as outlined in HB 1398. Students may elect to enroll in offered classes during the 2024-2025 school year as a transitionary phase. However, during the 2025-2026 school year it will be required and dedicated time will be set aside in the master schedule. Discussions leaned towards requiring the full credit during students' senior year due to flexibility in their schedule. However, if students have completed the computer science and cybersecurity requirement prior to their senior year, they may enroll in more elective courses to fill their school day.

The school Library Media Specialist will also curate a collection of books and other resources to cover cybersecurity and programming topics at appropriate levels for students. The school will provide access to these resources in the library and may promote their use through displays, book talks, and during elementary library specials.

When the master schedule includes STEM courses, the qualified educator teaching the course may incorporate cybersecurity and programming into the lessons. This can provide students with valuable skills and knowledge in these critical fields and provides additional exposure to cybersecurity and programming, in addition to graduation requirements.

With all described changes, students will be educated on all updated graduation requirements during the registration process with the counselor and school principal. Social media posts, letters, and reminders will be disseminated to educate all stakeholders and create a smooth transition.

**Notes**

- One credit required to graduate beginning 2025-2026.
- Depending on teacher qualifications, a mathematics courses could qualify and satisfy the full cybersecurity/programming credit needed for graduation and visa versa.
- Courses must be offered every year and can be completed through a Career and Tech Center, Regional Education Association, or through the North Dakota Center for Distance Education, unless requiring graduation credit.
- Integration plans must be embedded in curriculum for grades K-8.
- Graduation requirement waves integration plan for grades 9-12.

**School Board Approval**

The proposed integration plan will be presented to the board of education for potential approval during the April 2024 meeting. Information may be provided acknowledging potential costs to incur including professional leave for those who must attend training and earn certifications to teach and acquisition of hardware, software, and curriculum resources.

**Conclusion**

By implementing this Computer Science and Cybersecurity Integration Plan, Starkweather Public School District aims to empower students with the knowledge, skills, and resources needed to succeed in an increasingly digital world. Through collaborative efforts and a commitment to excellence in education, we aspire to prepare students to become responsible digital citizens and future leaders in technology and cybersecurity.

**This plan is developed in accordance with HB 1398 for the State of North Dakota and will be reviewed and updated periodically to ensure its effectiveness and relevance.

**Standards, Concepts, Topics, Lesson Ideas Grades K-6**

Kindergarten:

1. Online Safety Story Time: Host story time sessions focused on books that introduce basic online safety concepts in a kid-friendly manner. Choose books that teach about not sharing personal information, recognizing trusted websites, and asking a trusted adult for help online.
2. Digital Citizenship Puppets: Create simple puppets or use stuffed animals to act out scenarios related to digital citizenship and online safety. Use the puppets to role-play situations like asking permission before using someone else's device or being kind to others online.
3. Interactive Digital Citizenship Posters: Create interactive posters that teach kindergarten students about basic digital citizenship concepts, such as being safe, responsible, and respectful online. Include simple activities like matching pictures of safe online behaviors or identifying personal information.
4. Online Safety Songs and Rhymes: Write and perform catchy songs or rhymes about online safety and cybersecurity concepts. Use simple melodies and repetitive lyrics to help students remember important safety rules, such as "Only share with care, be safe and aware!"
5. Coding Storybooks: Introduce basic programming concepts through storybooks that feature characters learning about coding and problem-solving. Look for books that use age-appropriate language and illustrations to teach concepts like algorithms, sequences, and loops.
6. Hands-On Coding Activities: Provide hands-on coding activities using simple materials like building blocks, puzzles, or coding toys designed for young children. Encourage students to explore concepts like sequencing, patterns, and cause-and-effect through play-based learning experiences.
7. Digital Citizenship Games: Develop or adapt educational games that reinforce digital citizenship and online safety concepts. Create simple board games or interactive digital games that teach students about identifying safe websites, protecting personal information, and making responsible choices online.
8. Parent Workshops: Offer workshops or information sessions for parents on topics related to digital literacy, online safety, and cybersecurity for young children. Provide resources, tips, and strategies for parents to support their child's digital learning and safety at home.
9. Internet Safety Coloring Sheets: Create coloring sheets featuring characters or scenarios related to internet safety and cybersecurity. Use these coloring activities as a fun way for kindergarten students to reinforce key safety messages while developing fine motor skills.
10. Digital Citizenship Pledge: Engage kindergarten students in creating a classroom digital citizenship pledge or poster. Together, brainstorm and discuss simple rules for using

technology safely and respectfully, and encourage students to sign or decorate the pledge as a commitment to being good digital citizens.

Grade 1:

1. Online Safety Rules: Reinforce basic online safety rules, such as not sharing personal information, not talking to strangers online, and always asking an adult for help when encountering something unfamiliar online.
2. Safe and Unsafe Websites: Teach students to recognize safe websites by looking for trusted logos and avoiding unfamiliar websites.
3. Password Protection: Introduce the importance of creating strong passwords and explain that passwords should not be shared with anyone except trusted adults.
4. Device Safety: Teach students how to safely use electronic devices, including proper handling, charging, and turning devices off when not in use.
5. Cyberbullying Awareness: Introduce the concept of cyberbullying and teach students what to do if they encounter or witness cyberbullying, including reporting it to a trusted adult.

Grade 2:

1. Personal Information Protection: Emphasize the importance of keeping personal information private online and offline, including full name, address, phone number, and passwords.
2. Online Communication: Teach students about safe online communication practices, such as using polite language, avoiding sharing personal information in public forums, and being respectful to others online.
3. Privacy Settings: Introduce the concept of privacy settings on websites and apps and teach students how to adjust settings to control who can see their information.
4. Recognizing Scams: Teach students to recognize common online scams, such as phishing emails or messages, and to avoid clicking on suspicious links or providing personal information.
5. Reporting Concerns: Reinforce the importance of reporting any online activity that makes students feel uncomfortable or unsafe to a trusted adult.

Grade 3:

1. Digital Footprint: Introduce the concept of a digital footprint and explain that everything students do online leaves a trace. Teach students to think before they post and to consider the potential consequences of their online actions.
2. Safe Search Practices: Teach students how to conduct safe searches online, including using age-appropriate search engines, avoiding inappropriate content, and recognizing credible sources.
3. Privacy and Permission: Discuss the importance of respecting others' privacy online and obtaining permission before sharing someone else's photos, videos, or personal information.

4. Cybersecurity Threats: Introduce students to different types of cybersecurity threats, such as malware, viruses, and online scams, and teach them how to protect themselves from these threats.
5. Critical Thinking Online: Teach students critical thinking skills to evaluate online content critically, including distinguishing between fact and opinion, recognizing bias, and verifying information from multiple sources.

Grade 4:

1. Digital Citizenship: Teach students about the rights and responsibilities of digital citizenship, including respecting copyright laws, practicing ethical online behavior, and contributing positively to online communities.
2. Social Media Safety: Discuss the risks and benefits of using social media and teach students how to use social media safely, including setting privacy controls, managing friend lists, and avoiding sharing personal information publicly.
3. Online Gaming Safety: Teach students about online gaming safety, including setting privacy settings, avoiding sharing personal information with strangers, and practicing good sportsmanship.
4. Data Privacy: Introduce the concept of data privacy and teach students how their personal information is collected, used, and protected online by websites and apps.
5. Cyber Ethics: Discuss ethical considerations related to technology use, including issues such as online bullying, plagiarism, copyright infringement, and digital citizenship.

Grade 5:

1. Cybersecurity Basics: Teach students fundamental cybersecurity concepts, including the CIA triad (confidentiality, integrity, availability), encryption, authentication, and cybersecurity best practices.
2. Privacy Rights and Responsibilities: Discuss students' privacy rights and responsibilities online, including understanding privacy policies, controlling personal information, and advocating for privacy rights.
3. Safe Online Shopping: Teach students how to shop safely online, including using secure websites, protecting payment information, and recognizing online shopping scams.
4. Digital Literacy: Develop students' digital literacy skills, including effective search strategies, evaluating online sources for credibility and bias, and understanding how algorithms influence search results and recommendations.
5. Internet Safety Pledges: Encourage students to create and sign internet safety pledges, committing to responsible and safe online behavior, protecting personal information, and promoting digital citizenship.

Grade 6:

1. Cybersecurity Workshops: Organize cybersecurity workshops or guest speaker sessions for grade 6 students to learn about online safety, privacy protection, and cybersecurity threats. Invite experts or community members to discuss topics such as password security, social media safety, and protecting personal information online.

2. Programming Clubs: Establish programming clubs or coding workshops where grade 6 students can learn basic coding languages, such as Scratch or Python. Provide hands-on activities and projects that introduce programming concepts like algorithms, loops, variables, and conditional statements.
3. Digital Literacy Projects: Assign digital literacy projects that require grade 6 students to research, analyze, and present information on topics related to cybersecurity, internet safety, and digital citizenship. Encourage students to create multimedia presentations, infographics, or educational videos to share their findings with their peers.
4. Online Safety Games: Introduce online safety games or interactive simulations that challenge grade 6 students to navigate real-world scenarios related to cybersecurity and internet safety. Use gamified learning platforms or educational apps to engage students in problem-solving and critical thinking activities.
5. Cybersecurity Debates: Organize cybersecurity debates or discussions where grade 6 students can explore and debate various issues related to cybersecurity, such as online privacy rights, data breaches, social media ethics, and the impact of technology on society. Encourage students to research and present evidence to support their arguments.
6. Programming Projects: Assign programming projects that allow grade 6 students to apply their coding skills to real-world problems or challenges. Challenge students to design and create interactive games, animations, or multimedia presentations using coding languages or software development tools.
7. Cybersecurity Awareness Campaigns: Task grade 6 students with creating cybersecurity awareness campaigns or public service announcements (PSAs) to educate their peers and the school community about online safety and cybersecurity best practices. Encourage students to use creative mediums like posters, videos, or social media posts to spread awareness and promote positive digital habits.
8. Ethical Hacking Simulations: Introduce grade 6 students to ethical hacking simulations or cybersecurity challenges where they can practice identifying and mitigating security vulnerabilities in simulated environments. Provide opportunities for students to collaborate and problem-solve as they work to secure digital systems and protect against cyber threats.
9. STEM Career Exploration: Invite guest speakers from STEM fields, such as cybersecurity professionals, software engineers, or information technology specialists, to share their career experiences and insights with grade 6 students. Encourage students to explore STEM career pathways related to cybersecurity and programming through hands-on activities and career exploration resources.
10. Digital Citizenship Reflections: Facilitate discussions or reflective activities where grade 6 students can explore the ethical implications of technology use and reflect on their roles as responsible digital citizens. Encourage students to consider the impact of their online actions and to develop strategies for promoting positive digital behaviors within their communities.