The Culture of Technology 5

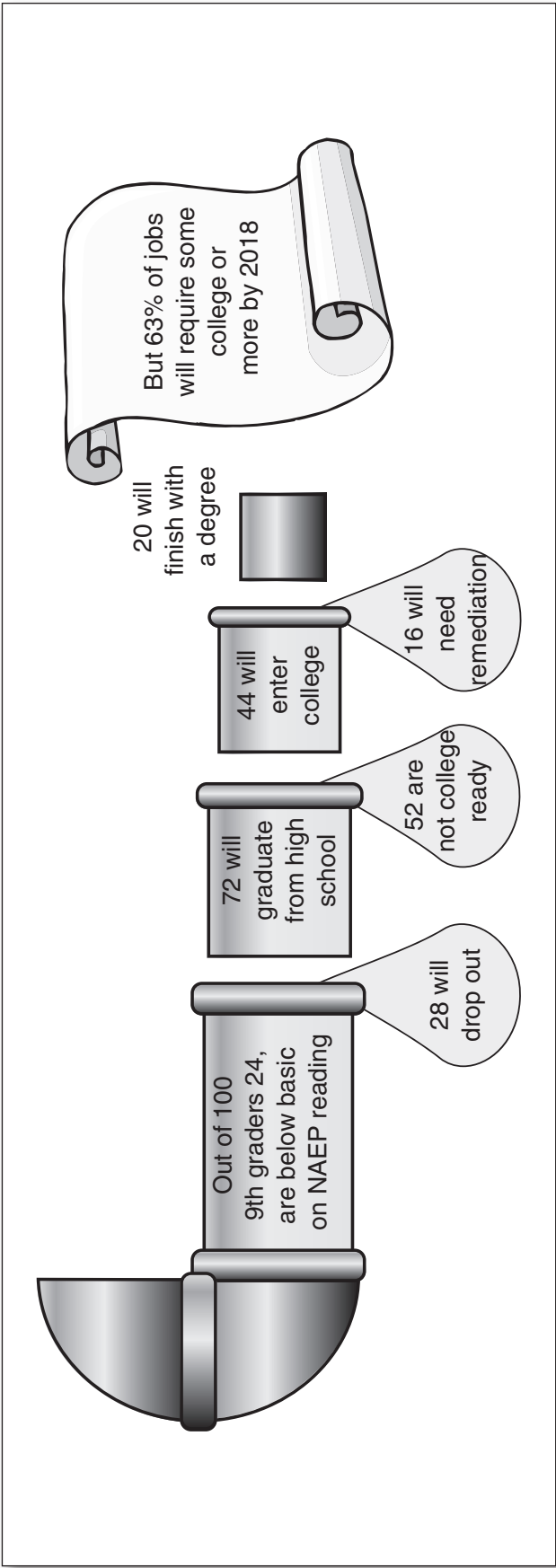## THE PRINCIPAL AS THE BUILDER OF TECHNOLOGY CULTURE

Beyond the reality of having the actual technological devices and systems in public schools, school administrators should be aware of a new educational culture and responsibility that come with 21st century learning and schools. As was discussed in Chapter 4, one of the core realities associated with 21st century learning is that technology is interwoven into the educational experience and that there is a close relationship among technology, pedagogy, and the content. Consequently, if school administrators get too focused on the "tools" of technology, they will be missing out on the essence of 21st century learning. In this new educational paradigm, educators are helping their students with developing essential competencies, dispositions, and literacies that will enable students to navigate an increasingly technological and changing world. Further considering the discussion in Chapter 8, we come to realize that we should not be basing our school infrastructure around a specific piece of technology but should instead be future-proofing our schools. This means that the actual infrastructure of the school is adaptable to changing devices and concepts of teaching, learning, and processing information. So too is the reality with students and technology. Twenty-first century learning is about helping young learners be adaptable and literate in the cultural, societal, and technological aspects of their world. It is not about the device itself, but more about the ability to be responsive, responsible, and innovative in technological use, no matter the device. This is the culture of technology, and school administrators, technology coordinators, and curriculum leaders have an integral responsibility in its creation.

The reality for schools that are integrating technology into school practices and educational activities is that the process is going to impact administrators, teachers, students, and families in both positive and negative ways. There is going to be excitement over the educational opportunities and the potential for real learning change. There is also going to be frustration over just how to incorporate technology into daily learning and how technology is actually going to be used in the classroom. It is one thing to have the vision for one-to-one learning, and it is another thing to plan it and do it. Educators need to embrace the opportunities and try to be creative in working through the frustrations because the educational reality is that 21st century learning is really not a choice. It is educational reform that needs to happen. Take a moment to reflect on Figure 5.1 from "The Digital Learning Imperative: How Technology and Teaching Meet Today's Education Challenges."

As a society, we cannot continue to lose this many students and have this many students ill-prepared for the needs of a 21st century economy. At the same time, students, as well as teachers, are genuinely excited about the learning opportunities that digital learning can bring. Research conducted by iTEC (Oldfield, 2012) found that there was a significant cultural and pedagogic change happening in the more than 1,200 classrooms surveyed across Europe. In the study, 85% of teachers reported that they felt confident in their digital technology skills. With this confidence, there was a solid connection established to the amount of time that technology was used in the classroom with 44% of the teachers reporting digital technology being used in 41% to 100% of their lessons. In addition, 56% of the teachers reported an increase in technology usage from their previous year of teaching. Of this increase in technology usage, teachers reported computer projection; digital resources such as e-books, databases; digital media tools such as video cameras, YouTube, Flickr; and text communication such as e-mail as their most used technologies. Of the most used technologies, 30.5% of teachers reported that computer projection technologies were very useful in aiding learning. Interactive whiteboards were rated second at 16.6%. Within this study, some 280,000 students were also surveyed about their ideas on technology in the classroom. The following list represents how students want to see technology in the classroom:

1. Schools provide students with netbooks.

2. Teachers focus on developing 21st century skills such as collaborative and social skills.

3. Schools provide students with digital exercise books and digital paper.

4. There is an increased focus on new media literacies.

Figure 5.1 The Leaking Pipeline

Out of 100 9th graders 24, are below basic on NAEP reading

28 will drop out

72 will graduate from high school

52 are not college ready

44 will enter college

16 will need remediation

20 will finish with a degree

But 63% of jobs will require some college or more by 2018

5. Schools increasingly teach specialist skills for specific jobs.

6. Schools provide unlimited access to the Internet when using a computer on school premises.

7. Pedagogies based on game design principles and play are increasingly seen as a tool for enjoying teaching and learning.

8. Learners work on projects, doing authentic tasks, and using technology creatively to tackle real challenges; this includes discovery-based learning.

9. Teachers use whole bodies of connected evidence from a variety of media to assess students.

10. Computers don't just present information but begin to understand its meaning. Intelligent systems learn what students are interested in and help them get what they want.

Notice in this list that it is not necessarily about the technology, but more about how they see the culture of learning in the classroom differently. Table 5.1 from the iTEC study portrays a real cultural shift in how the educational process is conceptualized when we bring technology, content, and pedagogy together.

Table 5.1 Taxonomy of Technology

Taxonomy	Category	Top Results
Activities and interactions (including pedagogy)	Curriculum and Assessment Knowledge and Skills	1. Teachers focus on developing 21st century skills such as collaborative and social skills. 2. There is an increased focus on new media literacies. 3. Schools increasingly teach specialist skills for specific jobs. 4. Pedagogies based on game design principles and play are increasingly seen as a tool for enjoying teaching and learning. 5. Learners work on projects, doing authentic tasks and using technology creatively to tackle real challenges; this includes discovery-based learning. 6. Teachers use whole bodies of connected evidence from a variety of media to assess students.
Environment	Learning Spaces	1. Learning spaces are designed to accommodate different learning activities.

Taxonomy	Category	Top Results
		2. Areas are set-up so that students can work as a team. The seating and table arrangement can be reconfigured to allow everyone to see and talk to each other.
		3. Schools have a variety of areas that can be used for lessons or study, including small spaces for individual work, small group working, and whole class teaching.
People and roles	Changing Roles	1. All learners have opportunities to work with other learners and to collaborate locally, nationally, and internationally.
		2. Learners are able to access formal education at any time of the day (people, resources, courses).
		3. There is an increase in child-centered learning with the teacher building links between children's interests and curricula.
Resources (including technology)	Technology	1. Schools provide students with netbooks.
		2. Schools provide students with digital exercise books and digital paper.
		3. Schools provide unlimited access to the Internet when using a computer on school premises.

When it comes to technology and learning, the researchers determined that students prefer more learner-centered and collaborative opportunities. Flexibility is also central in this learning cultural shift where students want flexibility in their learning spaces and also in terms of the how, when, and with whom learning can happen.

Drawing on this changing reality that both teachers and students are wanting and experiencing, principals will be integral in setting the direction for this technological cultural shift happening in schools around the world. The following material from *Leadership and Effectively Integrating Educational Technology* by Chris Toy (2008) describes 10 ways that principals can be instrumental in creating a 21st century culture of technology in their schools.

1. *Principals must effectively and consistently model the use of the same technology tools they expect teachers to use in their classrooms with students.* A powerful way for a principal to model the use of technology is to integrate it into staff meetings in the same way that teachers might in their classrooms.

2. *Principals must be consistent in their decisions and expectations about integrating learning technology in the school.* If a school faculty and administration agree to 21st century learning frameworks, there can be few exceptions to this integration. People will always be able to come up with excuses or rationalizations as to why they can't do it or need more time. Don't waiver in the vision

and the timeline. Granting exceptions just give justification that the previous way of doing things is still acceptable.

3. *The principal's communication about the pace and process of integrating learning technology needs to be clear and reasonable.* In your technology plan, make sure you are clear with your staff about just what you mean by "integrating technology" or by "digital learning." Clarity makes it much easier to set measurable and achievable goals for technology. This clarity also makes it easier for teachers to meet the technological targets you set.

4. *The principal must provide appropriate professional development time and resources to support effective classroom implementation technology.* Appropriate professional development sends a message to faculty that technology and 21st century learning are essential to the school reform process.

5. *The principal must support early adopters and risk takers.* You should be showing enthusiasm toward teachers who are genuinely interested in digital learning or one-to-one learning. This is the type of culture you want to encourage and support in your school. Get these teachers to share their efforts in staff meetings, or provide them with opportunities to attend technology workshops together.

6. *The principal must do whatever it takes to ensure that all staff has early access to the very same digital tools that students will be using in their classrooms.* The general guideline here is that teachers should have opportunities to use the new technology about 1 year to 6 months prior to integrating it into the classroom.

7. *As the educational leader, the principal must make it crystal clear to the technology coordinator that all decisions relating to learning technology will be made by the educational leaders with input from the technology leaders. Not the other way around. In the balance between control of the technology and access for learning, the more important consideration must be access for learning.* If, in the interest of safety and control, students are blocked from the technology and Internet access they need to truly change their learning, students and teachers will see little value in bringing technology into the classroom. In this sense, acceptable use policies are more important than extensive blocks and controls. The principal should establish a culture where staff and students know how to use technology responsibly.

8. *The principal must set and support the expectation that student work will be done and stored using technology.* Technology must be seen within the school as an integral component of how the work of education gets done. Principals must bring technology into the school culture in a way that makes education easier, more effective, or more engaging. If technology doesn't serve this role, then it will just be another burden placed on the shoulders of students and teachers.

9. *Principals must ensure that families and the public are kept informed about the school's goals and progress relating to its use of technology.* The promotional role of principals is essential in creating and establishing 21st century learning culture.

10. *The principal must be an active and public champion for all students, staff members, and the school in moving the vision of fully integrating learning technology*

for 21st century schools. Principals must continually articulate how technology integration and digital learning will benefit students and the learning process. Spotlight teachers who are exemplifying best practices and students who have used technology in meaningful and creative ways to improve their learning and achievement.

Rethinking the Concept of Technology Control

As technology becomes integrated into the 21st century learning experience, educational leaders are beginning to realize that we can no longer exist within a culture of technology control. The scope and variety of ways that technology is entering the learning process is just making this reality of technology control incredibly complex to manage and limits schools from reaching the full potential that new and innovative technologies can have on student achievement. The traditional approach for technology in schools was based on the paradigm of controlling where, when, and how students had access to technology. The computer lab is a prime example of this. On the other end of the spectrum, consider a program of Bring Your Own Device (BYOD) where students can use their own mobile devices to access the Internet through wireless systems in each classroom. In this educational paradigm, there is limited control, and students have anytime-anywhere access to technology and their learning.

The reason that control with technology exists in schools is because there is both a legal and philosophical responsibility to make sure our students are safe. Heavy protection features existed on computers to make sure that students did not use technology in inappropriate and possibly malicious ways. Teachers and administrators wanted to make sure that students stayed on task and focused on only using technology for purely academic purposes. This is called protection, or safety, and will be discussed in the section on culture of responsible use later in this chapter.

Reflecting back on many of the discussions in this book about technology, it is near to impossible to have the same culture of technology control. Twenty-first century learning requires a dramatic shift in how we conceptualize technology culture and how schools should be controlling it. Think closely as to why so many district and local school leaders are hesitant of bringing wireless technology into their schools and then allowing students to access the Internet in their classes through their own mobile devices? Why does this fear exist? Most readers would get the sense that educators are giving up a control feature that was inextricably linked to the culture of technology in schools. The culture was that we couldn't trust students to be responsible in how they used technology, what they were accessing on the mobile devices, and how they would be using these wireless devices in the classroom. Since educators couldn't trust students on the vast and expansive World Wide Web with all its dangers, we had to control students in how they used and accessed technology. This culture of technology presents itself in policies that prohibit broad categories of behavior and access: banning cell phones, blocking social networking sites, filtering certain topics or words. Taken to an extreme, these polices can lead to results ranging from humorous (one student was unable to do a report on his Congressman, Dick Armey, due to a key-word filter) to truly restrictive (where in some districts, teachers and students can

only use online services that have been approved with the district) (Massachusetts Educational Technology Advisory Council, 2010, p. 2).

Now this is not necessarily a bad thing because the intent behind this technology control has noble purposes. The issue at hand is that technological advances and the changing culture inherent in 21st century learning are demanding a shift in how educators conceptualize control and what it should look like.

In order to develop young learners who are inventive, inspired, and independent, educators need to create a culture of technology that gives them the freedom and respect to use technology and develop a digital literacy that is meaningful to them—not a culture that is derived from a limited technology perspective grounded in fear and control. So what would this 21st century concept of technology control look like?

- We can and should allow students to manage their own devices. Help them learn the relevant technical and organizational skills, especially as this has become a vital part of life outside school.
- Loosen the Parental Controls. Allow them the freedom and responsibility to manage their school apps, set up their school e-mail, and more. Have someone instruct them on best practices.
- Allow them the freedom to find and use other apps as appropriate to their activities in class.
- You can purchase some apps centrally but otherwise ask parents to purchase the apps. There is an abundance of inexpensive choices.
- A Responsible Use policy should clearly state what is allowed and disallowed. Child and parent alike should sign the policy.
- Freedom and responsibility come with consequence. Define a clear outcome for inappropriate use and act upon it as required.
- Use a Web filter but set restrictions loosely and only block categories of sites that are potentially harmful. Ensure you have monitoring in place so you can track Web usage if needed. Rather than acting as Big Brother, set an expectation of personal responsibility and take action when the standards are not met.
- Allow students the latitude to express their knowledge in different ways and with different tools wherever possible and subject to your prior approval. The process of learning should be more personally meaningful and motivational.
- Let them find and bring tools that they are most comfortable using.
- Give them the latitude to be teachers as well as learners: when they invent, discover, or master something new, have them teach others and create tutorials that you post online. (Gliksman, 2012)

Regardless of the varying level of controls that schools are setting regarding technology use, students are using technology extensively in both their educational and personal lives. We have moved out of the era where, for most students, the only access they had to technology was in the school. Take a look at Graphs 5.1 and 5.2 and the revealing data (n = 330,117 K–12 students) regarding student access to technology in our current context.
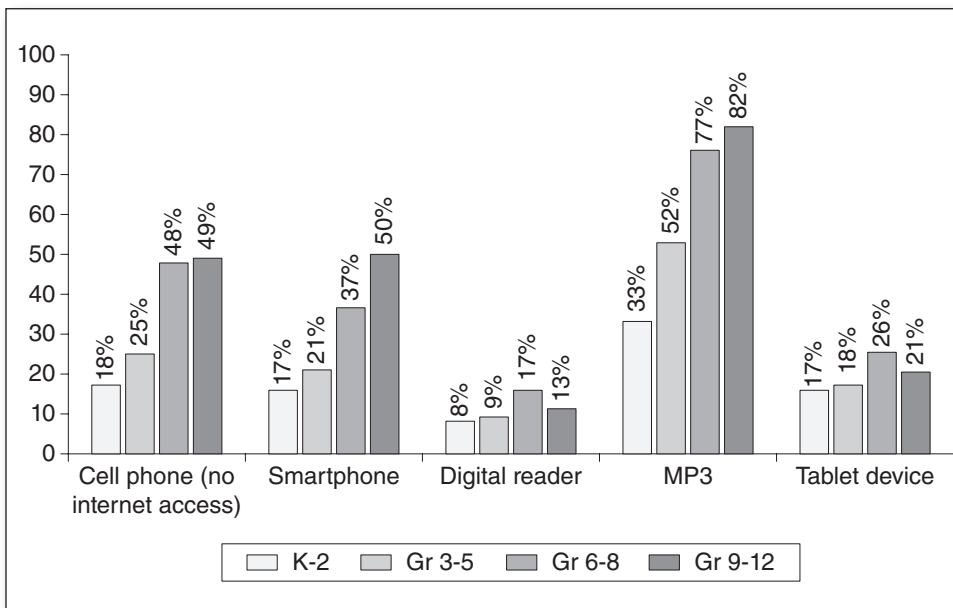
Graphic 5.1 High School Internet Access Outside of School
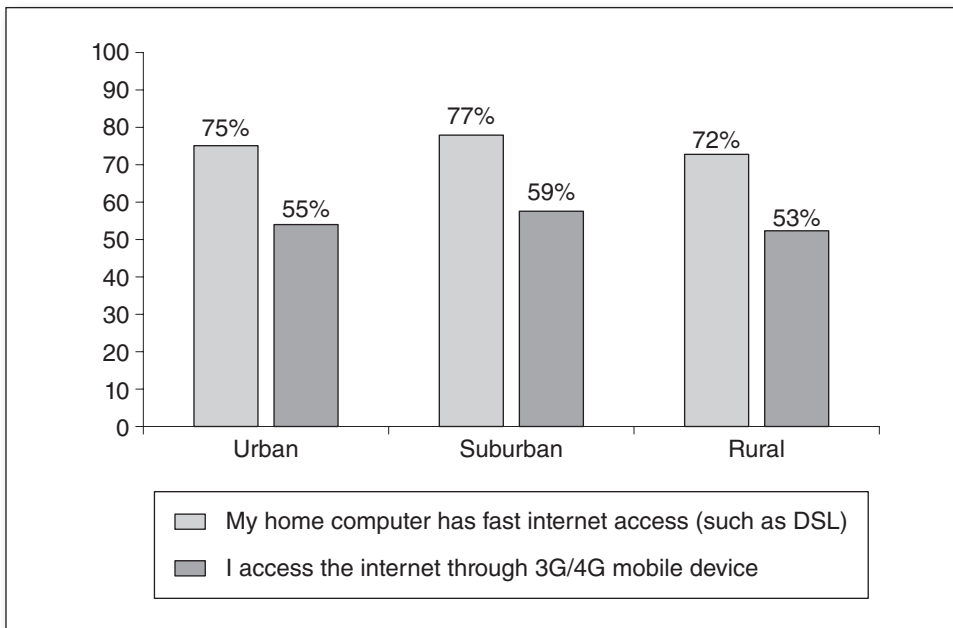
Source: Speak Up 2012. (2012). Mapping a personalized Learning Journey: K–12 students and parents connect the dots with digital learning. Retrieved from http://www.tomorrow.org/speakup/pdfs/SU11_PersonalizedLearning_Students.pdf

Graphic 5.2 Students' Personal Access to Mobile Devices

Source: Speak Up 2012. (2012). Mapping a personalized Learning Journey: K–12 students and parents connect the dots with digital learning. Retrieved from http://www.tomorrow.org/speakup/pdfs/SU11_PersonalizedLearning_Students.pdf

Students are not only using technology for personal use but also for educational purposes outside of school. In the study cited from the tables just presented, students indicated the following information.

- One in 10 students in Grades 6–12 have sent out a tweet about an academic topic that interests them.
- 15% have informally tutored other students online or found an expert to help them with their own questions.
- 18% have taken an online assessment to evaluate their own self-knowledge.
- One-fifth has used a mobile app to organize their schoolwork.
- One in four has used a video that they found online to help with homework.
- 30% of middle school students and 46% of high school students have used Facebook as a way to collaborate on classroom group projects.
- Almost half of high school students have sought out information online to help them better understand a topic that is being studied in class.

Students are showing educators that they can use technology as a part of their self-directed learning. In order for schools to provide that rich, digital experience that students need, the concept of control has to synchronize with the technological requirements of 21st century learning and to be more in line with how students are actually acting out their learning. Table 5.2 lists the areas of technology control that students saw as a problem, as presented in the Project Tomorrow study (Speak Up 2012, 2012).

Table 5.2 Student Perceived Barriers to Technology Use in Schools

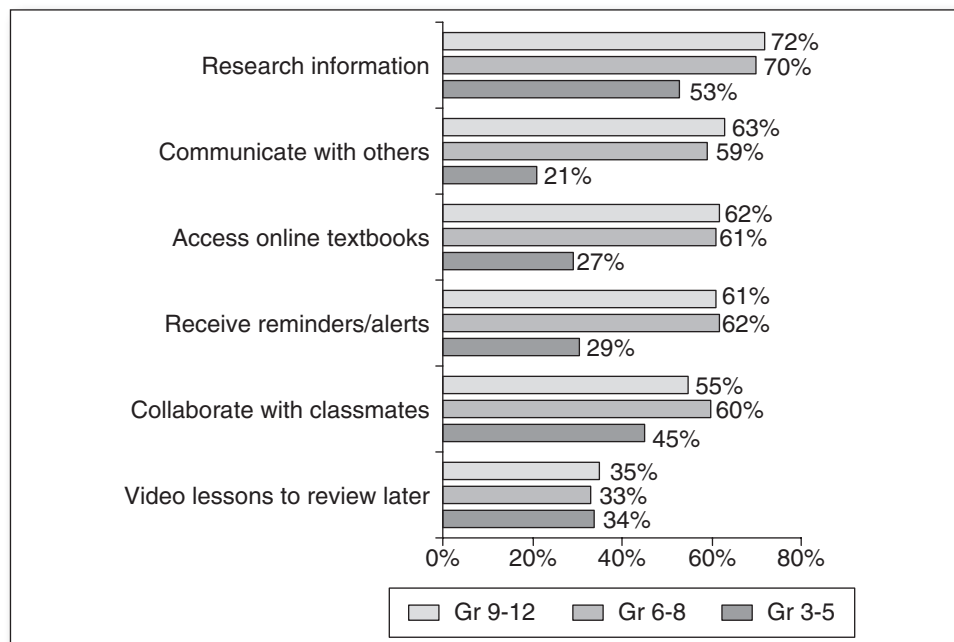| Obstacles to Tech Use at School	Students: Grade 6–8	Students: Grade 9–12
I cannot use my own mobile devices.	57%	55%
I cannot access my social networking site.	50%	51%
Websites I need for learning are blocked.	49%	59%
I cannot use my communications tools.	42%	39%
Teachers limit how I can use technology.	40%	42%

These students are telling educators that in setting up restrictive controls on technology usage, educators are limiting their learning potential. The students

were also questioned about what would be their wish list regarding technology use at school. The suggestions were the following:

- 47% of students wanted unlimited Wi-Fi Internet access throughout the school.
- 38% would like technological tools to help organize their schoolwork.
- 37% asked for access to the school network from home, school, or wherever they were with their mobile device.
- 36% of students wanted communications tools to support their interactions with other students and their teachers.
- 32% would like collaboration tools to work with their classmates on schoolwork projects.

Within this study, there was a great deal of discussion about mobile learning and digital learning through access with mobile devices. The students in this study want to bring mobile devices into the school and classroom and recognize that there will be many benefits to their learning due to the ease of access to content information, collaboration opportunities, and organizational infrastructures. The question for educators is whether or not we are ready to operate under a new concept of technological control that would open up these kinds of learning opportunities for students and teachers. Graph 5.3 presents a picture of how students would use mobile devices in their learning.

Graphic 5.3 Personalized Learning Through Mobile Devices at School

Research information — Gr 9-12: 72%, Gr 6-8: 70%, Gr 3-5: 53%
Communicate with others — Gr 9-12: 63%, Gr 6-8: 59%, Gr 3-5: 21%
Access online textbooks — Gr 9-12: 62%, Gr 6-8: 61%, Gr 3-5: 27%
Receive reminders/alerts — Gr 9-12: 61%, Gr 6-8: 62%, Gr 3-5: 29%
Collaborate with classmates — Gr 9-12: 55%, Gr 6-8: 60%, Gr 3-5: 45%
Video lessons to review later — Gr 9-12: 35%, Gr 6-8: 33%, Gr 3-5: 34%
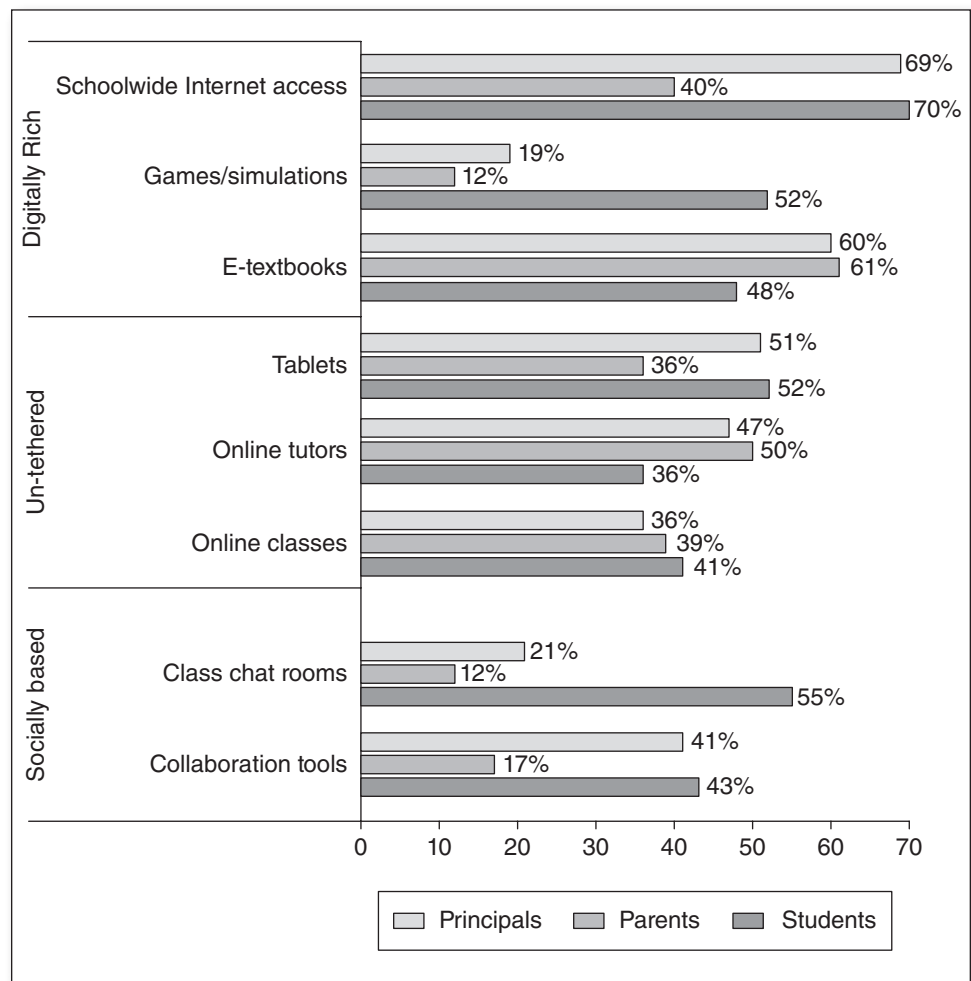
Legend: Gr 9-12, Gr 6-8, Gr 3-5

Source: Speak Up 2012. (2012). Mapping a personalized Learning Journey: K–12 students and parents connect the dots with digital learning. Retrieved from http://www.tomorrow.org/speakup/pdfs/SU11_PersonalizedLearning_Students.pdf

As a final picture of this changing culture of technology control in schools, the researchers in the Project Tomorrow study asked parents, students, and principals to conceptualize their ideal model for bringing technology into the school. In looking at Graph 5.4, readers will begin to see that due to the digital, wireless, and social network realities of this technology, traditional forms of technology control would make this technology reality near to impossible. In this sense, educators need to ask themselves about how they can rethink the way technology is controlled in their school so that 21st century learning can happen.

A New Culture of Digital Citizens

Reflecting on the discussion in the previous section, it is apparent that technology safety and control is shifting from being the sole responsibility of school administrators, teachers, and technology coordinators to a model of shared

Graphic 5.4 School Technology Wish List

Source: Speak Up 2012. (2012). Mapping a personalized Learning Journey: K–12 students and parents connect the dots with digital learning. Retrieved from http://www.tomorrow.org/speakup/pdfs/SU11_ PersonalizedLearning_Students.pdf

responsibility among educators, students, and families. This is directly in line with the philosophical basis of 21st century learning where the educational focus is on helping students to become digitally literate. In one sense, they become digital learners who are aware of and understand the norms of appropriate and responsible technology use. Taking it further, technology and academic plans in schools should address helping young learners to become digital citizens. The authors of this book have done extensive reading and discussion with colleagues on this topic. The following information represents a solid framework and guide for creating a culture of digital citizenry with the students in your school.

Nine Themes of Digital Citizenship (digitalcitizenship.net)

1. *Digital Access: Full Electronic Participation in Society.* Technology users need to be aware of and support electronic access for all to create a foundation for digital citizenship. Digital exclusion of any kind does not enhance the growth of users in an electronic society. All people should have fair access to technology no matter who they are. Places or organizations with limited connectivity need to be addressed as well. To become productive citizens, we need to be committed to equal digital access.

2. *Digital Commerce: Electronic Buying and Selling of Goods.* Technology users need to understand that a large share of market economy is being done electronically. Legitimate and legal exchanges are occurring, but the buyer or seller needs to be aware of the issues associated with it. The mainstream availability of Internet purchases of toys, clothing, cars, food, etc. has become commonplace to many users. At the same time, an equal amount of goods and services that are in conflict with the laws or morals of some countries are surfacing (which might include activities such as illegal downloading, pornography, and gambling). Users need to learn about how to be effective consumers in a new digital economy.

3. *Digital Communication: Electronic Exchange of Information.* One of the significant changes within the digital revolution is a person's ability to communicate with other people. In the 19th century, forms of communication were limited. In the 21st century, communication options have exploded to offer a wide variety of choices (e.g., e-mail, cellular phones, instant messaging). The expanding digital communication options have changed everything because people are able to keep in constant communication with anyone else. Now everyone has the opportunity to communicate and collaborate with anyone from anywhere and anytime. Unfortunately, many users have not been taught how to make appropriate decisions when faced with so many different digital communication options.

4. *Digital Literacy: Process of Teaching and Learning About Technology and the Use of Technology.* While schools have made great progress in the area of technology infusion, much remains to be done. A renewed focus must be made on what technologies must be taught as well as how they should be

used. New technologies are finding their way into the workplace that are not being used in schools (e.g., videoconferencing, online sharing spaces such as wikis). In addition, workers in many different occupations need immediate information (just-in-time information). This process requires sophisticated searching and processing skills (i.e., information literacy). Learners must be taught how to learn in a digital society. In other words, learners must be taught to learn anything, anytime, anywhere. Business, military, and medicine are excellent examples of how technology is being used differently in the 21st century. As new technologies emerge, learners need to learn how to use that technology quickly and appropriately. Digital citizenship involves educating people in a new way—these individuals need a high degree of information literacy skills.

5. *Digital Etiquette: Electronic Standards of Conduct or Procedure.* Technology users often see this area as one of the most pressing problems when dealing with digital citizenship. We recognize inappropriate behavior when we see it, but before people use technology, they do not learn digital etiquette (i.e., appropriate conduct). Many people feel uncomfortable talking to others about their digital etiquette. Often rules and regulations are created or the technology is simply banned to stop inappropriate use. It is not enough to create rules and policy, we must teach everyone to become responsible digital citizens in this new society.

6. *Digital Law: Electronic Responsibility for Actions and Deeds.* Digital law deals with the ethics of technology within a society. Unethical use manifests itself in the form of theft and/or crime. Ethical use manifests itself in the form of abiding by the laws of society. Users need to understand that stealing or causing damage to other people's work, identity, or property online is a crime. There are certain rules of society that users need to be aware of in an ethical society. These laws apply to anyone who works or plays online. Hacking into others' information, downloading illegal music, plagiarizing, creating destructive worms, viruses or creating Trojan Horses, sending spam, or stealing anyone's identify or property is unethical.

7. *Digital Rights and Responsibilities: Those Freedoms Extended to Everyone in a Digital World.* Just as in the American Constitution where there is a Bill of Rights, there is a basic set of rights extended to every digital citizen. Digital citizens have the right to privacy, free speech, etc. Basic digital rights must be addressed, discussed, and understood in the digital world. With these rights also come responsibilities as well. Users must help define how the technology is to be used in an appropriate manner. In a digital society, these two areas must work together for everyone to be productive.

8. *Digital Health and Wellness: Physical and Psychological Well-Being in a Digital Technology World.* Eye safety, repetitive stress syndrome, and sound ergonomic practices are issues that need to be addressed in a new technological world. Beyond the physical issues are those of the psychological issues that are becoming more prevalent such as Internet addiction. Users need to be taught that there inherent dangers of technology. Digital citizenship includes a culture

where technology users are taught how to protect themselves through education and training.

9. *Digital Security (Self-Protection): Electronic Precautions to Guarantee Safety.* In any society, there are individuals who steal, deface, or disrupt other people. The same is true for the digital community. It is not enough to trust other members in the community for our own safety. In our own homes, we put locks on our doors and fire alarms in our houses to provide some level of protection. The same must be true for the digital security. We need to have virus protection, backups of data, and surge control of our equipment. As responsible citizens, we must protect our information from outside forces that might cause disruption or harm.

Calgary Board of Education (CBE) Policy on Digital Learning

The following material represents how one school district is handling digital citizenry based on the nine themes of digital citizenship in their technology plan.

The following activities are prohibited and will be addressed on an individual basis as needed:

- Use of someone else's CBE account or access to the Learner Accessible Wireless Network (LAWN)
- Sharing of usernames and passwords for other people to use
- Sending, posting, displaying or using obscene language/messages or pictures or information about oneself or others
- Harassing, insulting, or attacking another person or their reputation
- Viewing websites through a proxy server
- Plagiarism of online content
- Texting or gaming
- Tampering with any computer accessories, hardware, or software
- Use of technology or accessing sites not approved by staff
- Trespassing in others' folders, work areas, or files
- Utilizing another student's device without permission
- The following sites are prohibited from use:
    - Vulgar or lewd depictions of the human body
    - Any adult content
    - Violent act
    - Online gambling
    - Social networking sites (such as Facebook, Nexopia, etc.)
    - Sites that encourage the use of illicit or illegal substances
    - Sites that advocate hatred or violence against an identifiable group
    - Sites promoting criminal activity
    - Noneducational games
    - And many more (see the link below for the complete list)

This is the specific CBE filter Level 2 (www.innovativelearning.ca/sec-learntech/POD/f2.html).

Our expectation is that our students will become educated and responsible digital citizens. If, however, students breach any of the above, each situation will be dealt with on an individual basis and may result in

- Restriction or loss of technology privileges
- Restriction of use or confiscation of personal device
- School based disciplinary consequences
- Police intervention and/or legal action

Lastly, it is important that parents/guardians and students remember the following as we begin this new educational opportunity:

- The school is not responsible for the loss, damage, or theft of student electronic devices.
- The school is not able to provide technical support for student devices.
- Devices can only be utilized when students are under the direct supervision of a teacher in an approved area of the school.
- Devices can only be utilized for educational purposes.
- Misuse will be determined by the staff and administration.

We view digital citizenship as a shared responsibility between students, their families, and the school. We appreciate families taking time to discuss this new opportunity with their children and supporting the work of the school in moving it forward. In discussing this matter at the family level, all students and families are to sign a Digital Citizenship Plan and return it to the appropriate school administrator. Each local school within CBE can adapt this based on specific local needs and student population variations.

Calgary Board of Education (CBE) Digital Citizenship Plan

In reviewing local digital citizenship plans, readers of this book can use this as a guide or a starting point for developing their own digital contract between students, families, and the school. Readers can also refer to Resource A at the end of this chapter for a graphic of a wireless network that is responsive to digital citizenry.

☐ I will make a plan with my parent(s)/guardian(s) around technology use (time, location, turning my phone off or leaving it in the kitchen at bedtime, online purchasing, etc.) at home.

  Plan Details:

  _____

☐ I understand that my phone and/or other tech device will be turned off at bedtime and I will not use it.

☐ I understand that we have an "open phone/technology" policy. That means my parent(s)/guardian(s) can review my calls, texts, e-mails, and/or _____ whenever they want.

☐ In my family, we always use passwords and we change them often. I will not give out my passwords to anyone—even best friends—other than my parent(s)/guardian (s).

☐ If a stranger ever contacts me or texts me, I will show my parents.

☐ I will not fight, swear, or gossip in e-mails or instant messages. I never respond to inflammatory, obscene, or insulting e-mails or to messages that are mean or in any way make me feel uncomfortable.

☐ If someone is mean to me online, I won't respond. I'll tell my trusted adult so we can make a plan to work together to solve the issue.

☐ If I see someone being mean to another person online, I will tell a trusted adult to get help.

☐ I will speak up and tell someone if I see something on the Internet that is wrong, inappropriate, or criminal in nature. I will be a good online citizen and not do anything that hurts other people or is against the law.

☐ I will not post or share personal pictures of myself or others on the Internet, by phone or

_____.

☐ We do not give out personal indentifying information such as our name, address, date of birth, school name, and/or phone number on a website or to people we meet online.

☐ If someone asks me something inappropriate when I am online, I understand that I need to tell my parent(s)/guardian(s). I also know I will not get in trouble and that telling my parent(s)/guardian(s) helps keep me safe and builds trust.

☐ I will not lie about my age to join any website and understand that the rules are designed to help keep me safe.

☐ I never download pictures, freeware, shareware, or text from unknown sources or websites we don't trust. I understand that plagiarism is cheating and pirating music, movies, and games is stealing.

☐ I will never open e-mail attachments from an unknown person or company. I do not follow links to websites through e-mail or click on pop-ups.

☐ I never respond to spam or junk mail. I keep my primary e-mail address only for use by my friends and family.

☐ I understand that there are consequences for not following these rules. Those consequences may include things like losing the privilege to use my phone or computer.

☐ I understand this digital citizenship plan is for my well-being and safety because my parent(s)/caregiver(s) love me.

☐ _____

☐ _____

☐ _____
☐ _____
☐ _____
☐ _____

_____   _____
Child's Signature   Parent's Signature

_____   _____
Date   Date

As part of this new initiative, the CBE has provided students and educators with a variety of resources to help in the integration of digital citizenry into the school culture. Readers can refer to the website listed for a complete list of their resources and their relevant URL links (www.cbe.ab.ca/learninginnovation/ digitalsafety-digitalcitizenship-mediaawareness.asp).

For the purposes of this book, some of the resources include:

Nine Elements of Digital Citizenship: a free Internet resource to support understanding of digital citizenship.

Privacy Pirates: Licensed website that is a game-based platform addressing concepts related to privacy and the Internet.

Passport to the Internet: Licensed website that is an interactive, role-playing resource to help in issues related to digital citizenship.

My World: Licensed website for high school students that includes Internet safety lessons, resources, activities, and games related to digital citizenship.

The Association for Media Literacy: A free Canadian resource for media literacy in education for teachers, parents, and students.
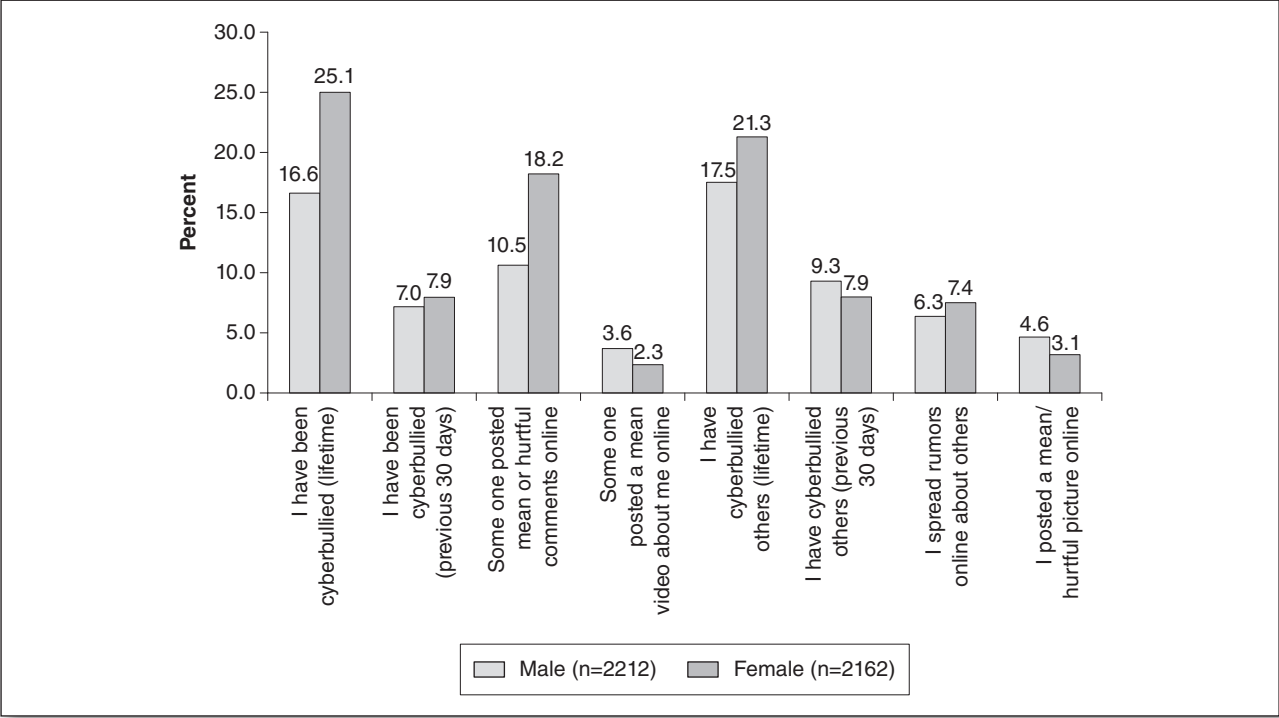
A Culture of Responsibility

As the shift of responsibility for safety and proper use of technology moves into a shared framework among educators, students, and families, school administrators have a variety of constructs they need to address in their schools. The following sections describe some of these cultural educational realities.

Cyberbullying

Cyberbullying is a growing concern among educators and parents. Cyberbullying is bullying that takes place using electronic technology. Electronic technology includes devices such as cell phones, computers, and iPads. It usually happens on communication tools such as social media sites, text messages, and information uploading sites like YouTube. Cyberbullying can take the form of mean/threatening text messages or e-mails, rumors, or gossip posted on social media sites, and/or embarrassing pictures or videos posted on websites. Graphs 5.5a and 5.5b describe the reality of cyberbullying among students.

Graphic 5.5a Cyberbullying by Gender

Legend: Male (n=2212) Female (n=2162)

Categories and values:
- I have been cyberbullied (lifetime): 16.6 / 25.1
- I have been cyberbullied (previous 30 days): 7.0 / 7.9
- Some one posted a mean or hurtful comments online: 10.5 / 18.2
- Some one posted a mean video about me online: 3.6 / 2.3
- I have cyberbullied others (lifetime): 17.5 / 21.3
- I have cyberbullied others (previous 30 days): 9.3 / 7.9
- I spread rumors online about others: 6.3 / 7.4
- I posted a mean/hurtful picture online: 4.6 / 3.1

Graphic 5.5b Cyberbullying by Offense

Categories and values:
- I have cyberbullied others (lifetime): 19.4
- I have cyberbullied others: 8.6
- One or more of the forms, two or more times: 11.2
- I posted mean or hurtful comments about someone online: 8.8
- I spread rumors about someone online, through text messages, or emails: 6.8
- I threatened to hurt someone through a cellphone text message: 5.4
- I threatened to hurt someone while online: 5.2
- I pretended to be someone else online and acted in a way that was mean or hurtful to them: 4.6
- I posted a mean of hurtful picture online of some one: 3.9
- I posted a mean or hurtful video online of someone: 3.1
- I created a mean or hurtful web page about someone: 2.9

previous 30 days

Source: Cyberbullying Research Center (2013).

Cyberbullying is real, and educators have a responsibility to create a culture of zero tolerance. There is a variety of resources available to help school administrators address this matter and develop a culture of respect and responsible technology usage among students. A great place to start is the website available at www.stopbullying.gov/cyberbullying/index.html or the National School Boards Association website. As an aid to principals and district leaders, the stopbullying.gov group conducted a review of state educational laws as they pertain to bullying. Their research indicated the following as core elements in a cyberbullying initiative. As a beginning point in establishing a culture of zero tolerance as it relates to cyberbullying, principals and educational leaders would benefit from making sure their current policies align with this infrastructure.

Cyber- and Antibullying Policy Framework

1. Purpose Statement

   a. Outlines the range of detrimental effects bullying has on students, including impacts on student learning, school safety, student engagement, and the school environment.

   b. Declares that any form, type, or level of bullying is unacceptable and that every incident needs to be taken seriously by school administrators, school staff (including teachers), students, and students' families.

   Example Statement:

   Oklahoma: Okla. Stat. Ann. Tit. 70, § 24–100.3 (2009): "The Legislature finds that bullying has a negative effect on the social environment of schools, creates a climate of fear among students, inhibits their ability to learn, and leads to other antisocial behavior. Bullying behavior has been linked to other forms of antisocial behavior, such as vandalism, shoplifting, skipping and dropping out of school, fighting, and the use of drugs and alcohol . . . Successful programs to recognize, prevent, and effectively intervene in bullying behavior have been developed and replicated in schools across the country. These schools send the message that bullying behavior is not tolerated and, as a result, have improved safety and created a more inclusive learning environment."

2. Statement of Scope: ***Covers conduct that occurs on the school campus, at school-sponsored activities or events (regardless of the location), on school-provided transportation, or through school-owned technology, or that otherwise creates a significant disruption to the school environment.***

   Example Statement:

   Indiana: Ind. Code Ann. § 20–33–8-13.5 (b) (2010), Disciplinary Rule Requirements: "The discipline rules [related to bullying] . . . must apply when a student is: (1) on school grounds immediately before or during school hours, immediately after school hours, or at any other time when the school is being used by a school group; (2) off school

grounds at a school activity, function, or event; (3) traveling to or from school or a school activity, function or event; or (4) using property or equipment provided by the school."

3. Specification of Prohibited Conduct

   a. Provides a specific definition of bullying that includes a clear definition of cyberbullying. The definition of bullying includes a nonexclusive list of specific behaviors that constitute bullying and specifies that bullying includes intentional efforts to harm one or more individuals, may be direct or indirect, is not limited to behaviors that cause physical harm, and may be verbal (including oral and written language) or nonverbal. The definition of bullying can be easily understood and interpreted by school boards, policymakers, school administrators, school staff, students, students' families, and the community.

   b. Is consistent with other federal, state, and local laws.

   c. Prohibited conduct also includes

       i Retaliation for asserting or alleging an act of bullying.

       ii Perpetuating bullying or harassing conduct by spreading hurtful or demeaning material even if the material was created by another person (e.g., forwarding offensive e-mails or text messages).

Example Statement:

Kansas: Kan. Stat. Ann. § 72–8256.C.2 (2009): "'Cyberbullying' means bullying by use of any electronic communication device through means including, but not limited to, e-mail, instant messaging, text messages, blogs, mobile phones, pagers, online games and websites."

4. Enumeration of Specific Characteristics

   a. Explains that bullying may include, but is not limited to, acts based on actual or perceived characteristics of students who have historically been targets of bullying and provides examples of such characteristics.

   b. Makes clear that bullying does not have to be based on any particular characteristic.

Example Statement:

North Carolina: N.C. Gen. Stat. § 115C-407.15(a) (2010): "Bullying or harassing behavior includes, but is not limited to, acts reasonably perceived as being motivated by any actual or perceived differentiating characteristic, such as race, color, religion, ancestry, national origin, gender, socioeconomic status, academic status, gender identity, physical appearance, sexual orientation, or mental, physical, developmental, or sensory disability, or by association with a person who has or is perceived to have one or more of these characteristics."

5. Development and Implementation of Local Education Agencies (LEA):
Directs every LEA to develop and implement a policy prohibiting bullying through a collaborative process with all interested stakeholders, including school administrators, staff, students, students' families, and the community, in order to best address local conditions.

   Example Statement:

   Maryland: Md. Code Ann., Educ. § 7–424.1(c) (2010): "[1] Each county board shall establish a policy prohibiting bullying, harassment, or intimidation. . . . [3] A county board shall develop the policy in consultation with representatives of the following groups: (i) Parents or guardians of students; (ii) School employees and administrators; (iii) School volunteers; (iv) Students; and (v) Members of the community."

6. Components of LEA

   a. ***Reporting of Bullying***

      iii Includes a procedure for students, students' families, staff, and others to report incidents of bullying, including a process to submit such information anonymously and with protection from retaliation. The procedure identifies and provides contact information for the appropriate school personnel responsible for receiving the report and investigating the incident.

      iv Requires that school personnel report, in a timely and responsive manner, incidents of bullying they witness or are aware of to a designated official.

   Example Statement:

   Wisconsin: Wis. Stat. § 118.46.1(a) (2009): "The [policy on bullying] shall include all of the following: . . . (6) A requirement that school district officials and employees report incidents of bullying and identify the persons to whom the reports must be made."

   b. ***Investigating and Responding to Bullying:*** Includes a procedure for promptly investigating and responding to any report of an incident of bullying, including immediate intervention strategies for protecting the victim from additional bullying or retaliation, and includes notification to parents of the victim, or reported victim, of bullying and the parents of the alleged perpetrator, and if appropriate, notification to law enforcement officials.

   Example Statement:

   Massachusetts: 2010 Mass. Adv. Legis. Serv. Ch. No. 71.370(g) (2010): "Upon receipt of such a report, the school principal or a designee shall promptly conduct an investigation. If the school principal or a designee determines that bullying or retaliation has occurred, the school principal or designee shall (i) notify the local law enforcement

agency if the school principal or designee believes that criminal charges may be pursued against a perpetrator; (ii) take appropriate disciplinary action; (iii) notify the parents or guardians of a perpetrator; and (iv) notify the parents or guardians of the victim, and to the extent consistent with state and federal law, notify them of the action taken to prevent any further acts of bullying or retaliation."

   c. ***Written Records:*** Include a procedure for maintaining written records of all incidents of bullying and their resolution.

Example Statement:

California: Cal. Educ. Code § 234.1 (2010): "The department shall assess whether local educational agencies have done all of the following: . . . (e) Maintained documentation of complaints and their resolution for a minimum of one review cycle."

   d. ***Sanctions:*** Include a detailed description of a graduated range of consequences and sanctions for bullying.

Example Statement:

Alabama: Ala. Code § 16.28B.5 (2010): "The model policy, at a minimum, shall contain all of the following components: . . . [4] A series of graduated consequences for any student who commits an act of intimidation, harassment, violence or threats of violence. Punishment shall conform with applicable federal and state disability, antidiscrimination, and education laws and school discipline policies."

   e. ***Referrals:*** Includes a procedure for referring the victim, perpetrator, and other to counseling and mental or other health services, as appropriate.

Example Statement:

Maryland: Md. Code. Ann., Educ. § 7–424.1.b (2010): "[2] The model policy . . . shall include: . . . (viii) Information about the types of support services available to the student bully, victim, and any bystanders . . . "

7. Review of Local Policies: ***Includes a provision for the state to review local policies on a regular basis to ensure the goals of the state laws are met.***

Example Statement:

Illinois: 105 Ill. Comp. Stat. Ann. 5/27–23.7(d) (2010): "The policy must be updated every 2 years and filed with the State Board of Education after being updated. The State Board of Education shall monitor the implementation of policies created under [this subsection of the statute]."

8. Communication Plan: ***Includes a plan for notifying students, students' families, and staff of policies related to bullying, including the consequences for engaging in bullying.***

Example Statement:

Arkansas: Ark. Code Ann. § 6–18–514(b) (2009): "The policies shall: [6] Require that notice of what constitutes bullying, that bullying is prohibited, and the consequences of engaging in bullying be conspicuously posted in every classroom, cafeteria, restroom, gymnasium, auditorium, and school bus in the district; and [7] Require that copies of the notice . . . be provided to parents, students, school volunteers, and employees."

9. Training and Preventative Education

   a. Includes a provision for school districts to provide training for all school staff, including, but not limited to, teachers, aides, support staff, and school bus drivers, on preventing, identifying, and responding to bullying.

   b. Encourages school districts to implement age-appropriate school- and community-wide bullying prevention programs.

   Example Statement:

   South Carolina: S.C. Code Ann. § 59–63–140 (F) (2009): "Schools and school districts are encouraged to establish bullying prevention programs and other initiatives involving school staff, students, administrators, volunteers, parents, law enforcement, and community members."

10. Transparency and Monitoring

    a. Includes a provision for LEAs to report annually to the state on the number of reported bullying incidents, and any responsive actions taken.

    b. Includes a provision for LEAs to make data regarding bullying incidence publicly available in aggregate with appropriate privacy protections to ensure students are protected.

    Example Statement:

    Ohio: Ohio Rev. Code Ann. § 3313.666.10 (2010): "the district administration . . . [shall] provide . . . a written summary of all reported incidents and post the summary on its website."

11. Statement of Rights to Other Legal Recourse: ***Includes a statement that the policy does not preclude victims from seeking other legal remedies.***

    Example Statement:

    Oregon: Or. Rev. Stat. Ann. § 339.364 (2009): "Victim may seek redress under other laws. . . . [This statute] may not be interpreted to prevent a victim of harassment, intimidation, or bullying or a victim of cyberbullying from seeking redress under any other available law, whether civil or criminal."

Source: "Key Components in State Anti-bullying Laws" (2013).

Cybersafety and Security

The Internet is an amazing place. It is also a dangerous place. Local and national news regularly cover stories related to hackers stealing personal information from computers and databases, or kids being lured into dangerous situations as a result of "meeting" someone in a chat room. Schools have always been responsible for the safety of students while they are in the care of educators. It is a social responsibility that teachers and school administrators take very seriously. In an environment of digital learning and regular technology usage, keeping students safe and secure while online is a very real concern. To this end, cybersafety is the ability to act in a safe and responsible manner when interacting online. It also includes digital behaviors that help students to protect their reputation and to protect their personal information. In establishing a culture of cybersafety in their schools, school administrators should engage their staff and students in a dialogue about cybersafety. School administrators and teachers can focus their discussion within the following areas:

- Talk with students about how to recognize online risks, make informed decisions, and take appropriate actions to protect themselves. This includes helping students know how to identify potentially dangerous online situations and how to appropriately avoid or report them: for example, posting offensive material, "friending" strangers, posting private information, and engaging in or failing to report cyberbullying.
- Talk with students about how to make informed decisions about appropriate protection methods and safe practices in a variety of online situations. This includes helping children understand the importance of following Terms of Use guidelines, disciplined and productive use of Internet time, safely exiting an inappropriate site, protection of passwords, and avoiding cyberbullying.
- Show students how to demonstrate and be an advocate for safe behaviors among peers, family, and community.

Source: Internet Keep Safe Coalition (2009).

Acceptable Use

Twenty-first century digital learning is going to naturally see students increase the amount of time accessing online resources and using school technology for their learning. Digital citizenship is so important because it helps students understand acceptable and responsible ways to use the technology. Acceptable use is basically a policy and a contract between the students and the school that the students will respect district and school technology resources.

The Department of Education in the State of Victoria in Australia has put together a sound template that school administrators can use in establishing necessary agreements between students and schools as it relates to acceptable use. School leaders can use this as a guide to establishing acceptable use practices in their school.

At [INSERT SCHOOL NAME] we

- Support the rights of all members of the school community to engage in and promote a safe, inclusive and supportive learning environment
- Have a Student Engagement Policy that clearly states our school's values and the expected standards of student behavior, including actions and consequences for inappropriate behavior
- Educate our students to be safe and responsible users of digital technologies
- Raise our students' awareness of issues such as online privacy, intellectual property, and copyright
- Supervise students when using digital technologies for educational purposes
- Provide a filtered Internet service but acknowledge that full protection from inappropriate content can never be guaranteed
- Respond to issues or incidents that have the potential to impact on the well-being of our students
- Know that some online activities are illegal, and as such, we are required to report this to the police
- Provide parents/guardians with a copy of this agreement
- Support parents/guardians to understand the importance of safe and responsible use of digital technologies, the potential issues that surround their use and strategies that they can implement at home to support their child

Acceptable Use Agreement: Upper Primary and Secondary Students

Cybersafety is an important issue for all students. By the time students arrive at secondary school, most will already be regular and active users of digital technologies including social media tools such as Facebook.

Schools that want to support students to behave safely and responsibly online, both inside and out of school, can use this agreement template. Schools can add and/or delete information to make them relevant to the school environment.

Students can work through the behaviors described in Part B at school with their teacher and take it home to share and discuss with their parents.

Part C is for schools that received funding to purchase devices through the National Secondary School Computer Fund (NSSCF). If the school did not receive funding, this section can be deleted.

Part A: School Profile Statement

[INSERT SCHOOL NAME] recognizes the need for students to be safe and responsible users of digital technologies. We believe that explicitly teaching students about safe and responsible online behaviors is essential and is best taught in partnership with parents/guardians. We request that parents/guardians work with us and encourage this behavior at home.

The school profile statement should focus on programs and procedures that are in place to support safe and responsible use of digital technologies. This statement can define how the school demonstrates their duty of care for students working in online spaces. This statement should be revised regularly to reflect a detailed understanding of the school's relevant programs and procedures as well as online needs of their students.

Part B: Student Declaration

When I use digital technologies I agree to be a safe, responsible, and ethical user at all times, by

- Respecting others and communicating with them in a supportive manner; never writing or participating in online bullying (for example,

forwarding messages and supporting others in harmful, inappropriate, or hurtful online behaviors)

- Protecting my privacy; not giving out personal details, including my full name, telephone number, address, passwords, and images
- Protecting the privacy of others; never posting or forwarding their personal details or images without their consent
- Talking to a teacher if I personally feel uncomfortable or unsafe online, or if I see others participating in unsafe, inappropriate, or hurtful online behaviors
- Carefully considering the content that I upload or post online; this is often viewed as a personal reflection of who I am
- Investigating the terms and conditions (e.g., age restrictions, parental consent requirements). If my understanding is unclear, I will seek further explanation from a trusted adult.
- Confirming that I meet the stated terms and conditions; completing the required registration processes with factual responses about my personal details
- Handling information and communications technology devices with care and notifying a teacher if they are damaged or require attention
- Abiding by copyright and intellectual property regulations. If necessary, I will request permission to use images, text, audio, and video and cite references.
- Not interfering with network systems and security, the data of another user or attempting to log into the network with a user name or password of another student
- Not bringing to school or downloading unauthorized programs, including games

In addition, when I use my personal mobile phone, I agree to be a safe, responsible, and ethical user at all times, by

- Respecting others and communicating with them in a supportive manner; never verbally or in writing participating in bullying (for example, harassing phone calls/text messages, supporting others in harmful, inappropriate, or hurtful online behaviors by forwarding messages)
- Keeping the device on silent during class times; only making or answering calls or messages outside of lesson times (except for approved learning purposes)
- Respecting the privacy of others; only taking photos or recording sound or video at school when I have formal consent or it is part of an approved lesson
- Obtaining appropriate (written) consent from individuals who appear in images or sound and video recordings before forwarding them to other people or posting/uploading them to online spaces

Part C: Conditions of Use for School-Owned Devices

Equipment

Ownership

- If taken home, the student must bring portable devices fully charged to school every day.
- The school retains ownership of the device until the student completes Year 12. At this time ownership of the device will be determined by the school.
- Parents/guardians and students should be aware that files stored on the device, or on the school's server, are not private.
- If the student leaves the school prior to completing Year 12 or moves to another government or nongovernment school, interstate or overseas, the device must be returned to the school.

Damage or Loss of Equipment

- All devices and batteries are covered by a manufacturer's warranty. The warranty covers manufacturer's defects and normal use of the device. It does not cover negligence, abuse, or malicious damage.
- Any problems, vandalism, damage, loss or theft of the device must be reported immediately to the school.
- In the case of suspected theft, a police report must be made by the family and a copy of the report provided to the school.
- In the case of loss or accidental damage, a statement should be signed by a parent/caregiver and provided to the school.
- Students may be required to replace lost or damaged chargers.
- If a device is damaged or lost, the principal or their nominee will determine whether replacement is appropriate and/or whether the student retains access to a device for home use.
- If a device is damaged and the damage is not covered by the manufacturer's warranty or any of the school's insurance arrangements, the principal may determine that the student will pay the costs of repairing the damage or, if necessary, the costs of replacing the device.

Standards for Device

The student is responsible for

- Adhering to the school's Acceptable Use Agreement or Student Engagement Policy when using the machine, both at home and school
- Backing up data securely
- Maintaining settings for virus protection, spam, and filtering that have been set as a departmental standard

Part D: Student Commitment

Definition of Digital Technologies

This Acceptable Use Agreement applies to digital technologies, social media tools, and learning environments established by our school or accessed using school-owned networks or systems, including (although are not limited to)

- School-owned information and communications technology devices (e.g., desktops, laptops, printers, scanners)
- Mobile phones
- E-mail and instant messaging
- Internet, Intranet, and Ultranet
- Social networking sites (e.g., Facebook, SuperClubsPLUS)
- Video and photo sharing websites (e.g., Picasa, YouTube)
- Blogs
- Microblogs (e.g., Twitter)
- Forums, discussion boards, and groups (e.g., Google groups, Whirlpool)
- Wikis (e.g., Wikipedia)
- Vod and podcasts
- Video conferences and Web conferences.

This Acceptable Use Agreement applies when I am using any of the above digital technologies at school, at home, during school excursions, camps, and extracurricular activities.

I understand and agree to comply with the terms of acceptable use and expected standards of behavior set out within this agreement. I understand that there are actions and consequences established within the [INSERT SCHOOL NAME] Student Engagement Policy if I do not behave appropriately.

Date: _____

Student Name: _____

Name of School Contact: _____

Phone Number of School Contact: _____

Parent/Guardian A Signature: _____

Name of Parent/Guardian A: _____

Parent/Guardian B Signature: _____

Name of Parent/Guardian B: _____

_____

© State of Victoria 2012

Source: Victoria Department of Education and Early Childhood Development (2013).

FUTURE CHALLENGES

An important part of 21st century learning and schools is recognizing that we are trying to develop a new culture as it relates to technology. This technology

culture happens through an articulate principle that creates it at the school level. This culture is about conceptualizing a new relationship between technology and school control. As the level of technology control shifts to a more free and open access to technology and information, a culture of digital citizenship will emerge. From here, digital citizenship requires that students learn to use technology and online activities in safe and responsible ways. As such, a culture of responsible use needs to be stipulated within technology school reform plans. The key concept here is that school administrators, technology coordinators, and curriculum leaders have to be careful that they don't just focus on the devices of technology plans. For 21st century schools and digital learning to be a success, the future challenge for educators is to blend the technology devices and infrastructures with an appropriately aligned technology culture.

REFLECTIVE ACTIVITIES

1. Describe how your school/district currently understands control as it relates to technology use.

2. Most educators have taken the time to write an educational/teaching philosophy statement. Write a technology philosophy statement. Readers may want to try the survey by Jason Ohler titled "Knowing your school's technology culture" (available at www.jasonohler.com/pdfs/anthro-tech-assess.pdf) to help you formulate your philosophy of technology as it relates to your school.

3. Assess your current Acceptable Use document. Is it meeting the current needs of your school and students based on your technology plan?

4. List three things you have done in the past 6 months to address cyberbullying in your school.

5. Look ahead and write down one new thing you can do in the next month to respond to a cybersafety issue with your students.

6. After reading this chapter, write down three things you are doing to help your students to become stronger digital citizens. Now describe two new things you would like to do in your school to help your students to be better digital citizens.

Wireless Infrastructure (Calgary Board of Education)

Guest Network

Allowing Schools to Control Who Uses Their Wireless Network

Web access has become fundamental to not only our students and staff, but to visiting guests at the schools. The CBE recognizes that guests such as parents, presenters, or private contractors may require Web access in order to enrich the learning environment we provide to our students. To this end, we have created a "Captive Portal" system similar to those you see when you go to a coffee shop or free access Wireless location.

Setting Up Guest Accounts:

The School Principal will be responsible for delegating individuals to administer wireless guest accounts. An administrator will log into the wireless system from a desktop computer, and will create a username and password for a guest user that requires access.

Using CBE Guest Accounts:

Once a guest account has been created, guests:
1. need to enable their wireless cards,
2. connect to the "CBE GuestNet" network.
3. will have to open a web browser,
4. browse to any website they wish.
5. will be presented with a login page.
6. will log in using their guest account information as set up by the school's assigned Administrator.

How Long and Where Do They Work?

Guest accounts can be valid from a minute to five days, and can only be used at the school which created the account. Accounts will automatically be disabled and removed from the system.

It is important to note that this guest accounts have less network access than the CBE Owned Devices network, and as such students/staff are discouraged from using this network for their web surfing requirements.

Network Overview

Three Networks

The CBE is deploying three networks

- one for CBE Owned Equipment,
- one for CBE Learners
- one for CBE Guests.

Each of these networks has different features and services. Some of these features are detailed in the chart below:

	CBE Owned Devices	CBE LAWN	CBE GuestNet
Internet Access	Standard	Limited	Limited
Content Filtering Level	School + Teacher level filtering	School level filtering only	School level filtering only
School LAN access	YES	NO	NO
Login Method	Automatic	Captive Portal using CBE login credentials	Captive portal using credentials created by school
Locations Usable	Every CBE School	Every CBE School	Only at the school where the account is created
Equipment	All CBE wireless devices	Staff and Student Devices only	Guest devices only

What if I need help?

If you have questions or require further information about your new Wireless infrastructure, please contact the HELP DESK. If you experience technical or performance problems with your new equipment, please contact the HELP DESK or have your School Tech raise a HEAT ticket that outlines the problem you are experiencing. We are committed to resoling your issues promptly.

Calgary Board of Education

Using CBE School Wireless

Why Use CBE Wi-Fi?

Available at all CBE Schools

The CBE recognizes the need to provide its digital citizens easy access to wireless connectivity for every one of our schools. Wireless access to the CBE network and to the Internet is a critical component of our three year education plan.

Simple

The CBE's Wireless eliminates the need to learn or share complex network passwords, and allows CBE equipment to easily connect to the network from any location. Using their existing CBE username and passwords Students and teachers will be able to connect their personal devices to the CBE Learner Accessible Wireless Network (CBE LAWN) at any site. In addition CBE guests such as contractors and parents will be able to access the Internet from accounts that the school will create and control.

Fast

The CBE's Wireless network infrastructure used legacy technologies, but has been expanded to include newer and faster 5Ghz 802.11n technologies.

Getting Started

All you need to get started is a device that has Wireless capability. This could be a laptop, netbook, iPod/iPhone, or any other device. Just check your owner's manual or look for the wi-fi logo on your device:

CBE Owned Devices

Secure Network Access to the CBE Network From Every School

The new network allows you to take your **CBE issued device** to any school and access all the network facilities at the location including printers, scanners, and file-shares/servers.

It is important to note that this level of access is only available to CBE equipment. Your personal computer or computers that your guests bring in will have to connect to either the CBE LAWN or the CBE Guest-Net networks.

In order to connect wirelessly, you need to complete this **one time procedure. Your school tech will be able to assist you if required:**

- Power down your device, and connect it to the school network using a blue cable.

- Boot up your device, and once it has fully booted, unplug it from the school network.

- Surf Wirelessly

After completing these steps **once**, you will be able to use the wireless CBE Owned Devices network at every school.

Please note that during the initial few months of this network rollout, Macintosh computers will require the school tech to configure the Mac before it will work on the LAWN.

CBE LAWN

(CBE Learner Accessible Wireless Network)

Wireless Internet to Every CBE Digital Citizen at Every School

In keeping with the philosophy of student lead learning at the CBE, **students and staff** will now be able to bring their own wireless devices to the school and access the Internet. The network will work with any wireless device that supports 802.11b/g/n technology.

Connecting to the Network:

1. enable your wireless card,
2. look for the "CBE LAWN" Network connect to it.
3. open your web browser browse to
4. any website you wish. You will be presented with a login page.
5. Simply login using your CBE username and password.
6. You will then be able to surf the web on that device.

When should I use this network?

You should use this network for your own personal devices only, and must not connect CBE owned computers to it. For example, the network will be content filtered to the level of the school you are at. Some websites may be blocked that would be accessible from with a CBE owned device. This network only allows for Web surfing, whereas the CBE Owned Devices network allows access to a broader range of services on the Internet.