Horizon School Division No. 67	**Policy Code:**	**HG**
	Policy Title:	Citizenship in a Digital Age
Policy Handbook	**Cross Reference:**	HGAO use of technology, HGAN technology resources, JB FOIP IHF Safe and Caring Schools
	Legal Reference:	
	Adoption Date:	June 18, 2013
	Amendment or Re-affirmation Date:	

POLICY

THE BOARD OF TRUSTEES OF HORIZON SCHOOL DIVISION BELIEVES IN THE USE OF TECHNOLOGY TO SUPPORT, ENGAGE, AND EMPOWER THE TEACHING AND LEARNING ENVIRONMENT. THE BOARD FURTHER RECOGNIZES THAT DIGITAL CITIZESHIP IS A FUNDAMENTAL COMPONENT OF CITIZENSHIP, THE LEARNING ENVIRONMENT, AND STUDENT COMPETENCIES.

DEFINITIONS

Learning Environments that Contain Technologies:

Technology and digital connectedness plays an important role in the learning community and citizenship in a digital age that encompass working, socializing, and learning in digitally enmeshed environments. While the focus of this policy is on the use of technology, it endorses a 'pedagogy-first' approach which emphasizes the way in which technology supports learning.

Citizenship in a Digital Age:

Citizenship is defined as the state of being a citizen of a particular social, political, national, and/or global community. Citizenship carries both rights and responsibilities. It requires ever-evolving morals, personal empowerment, meaningful participation, education, being inclusive, and is tied to community. Citizenship in a digital age extends citizenship to the digital context with a focus on the development of engaging thinkers, and creating ethical citizens with an entrepreneurial spirit. Citizenship in a digital age requires balancing personal empowerment and responsibility with community well-being and includes the following three components.

- Respect and Protect Yourself: Digital Well-being
- Respect and Protect Others: Digital Interactions
- Respect and Protect Intellectual Property and other Property: Digital Preparedness

GUIDELINES

1. The Board expects responsible, purposeful use of technology without compromising an individual's right to privacy, a welcoming, caring, respectful and safe learning environment, and the integrity of the teaching/learning environment.

2. Administrative guidelines shall be attached to the Policy for the purpose of outlining procedures relative to the policy including, but not limited to the following:

a) Citizenship in a Digital Age (Attachment #1)
b) Digital Rights and Responsibilities: Acceptable and Responsible Use (Attachment #2)
c) Protection of Personal Information (Attachment #3)
d) Communication: Social Media, Web-Based, Division Owned Vehicles (Attachment #4)
e) Connectivity: Wireless and Bring your own Device (Attachment #5)
f) Standard Operating Procedures (Attachment #6)

3. Schools shall develop "Citizenship in a Digital Age" policies that align with the guidelines outlined in this policy.

4. Schools shall foster a 21st Century Inclusive Learning Culture that provides rigorous, relevant, and engaging learning opportunities for all students and staff.

a. Promote access to appropriate digital tools and resources to meet the needs of all learners
b. Account for continuous improvement of 21st century learning competencies across the curriculum
c. Model and promote effective use of technology for learning
d. Promote and participate in local, national, and global learning communities that stimulate innovation, creativity, and 21st Century collaboration and competencies
e. Design and adapt relevant learning experiences that incorporate digital tools and resources to promote student learning, engagement, and creativity
f. Develop technology-enriched learning environments that facilitate differentiated instruction.

5 Jurisdiction students and staff model and facilitate understanding, commitment, and alignment of safe, social, ethical and legal issues and responsibilities related to citizenship in a digital age.,

6. The collection, storage, use, disclosure, disposal and destruction of personal information in digital form adhere to applicable regulations and laws including, but not limited to, the School Act, the Freedom of Information and Protection of Privacy Act, the Child Welfare Act, and the Income Tax Act.

ATTACHMENT #1

Horizon School Division # 67

CITIZENSHIP IN A DIGITAL AGE ADMINISTRATIVE GUIDELINES

CITIZENSHIP IN A DIGITAL AGE

Citizenship in a digital age encompasses a vast and ever changing topic that attempts to deal with and address respect protection of self, others, intellectual property and other property. The following administrative guidelines attempt to address the following topics.

Respect and Protect Yourself: Digital Well-being

1. Digital Security: Electronic precautions for self-protection
   a. Students and staff demonstrate a sound understanding of technology concepts, systems, and operations (see standard operating procedures).
      (1) Understand, select, and use technology systems and applications purposefully, appropriately, effectively, and productively
      (2) Transfer current knowledge to learning of new technologies
   a. Protection of Personal Information Guidelines and Procedures
      (1) Appropriate access
      (2) Risk vs. educational and business goals
      (3) Appropriate communication
      (4) Plagiarism, ownership, and responsibility (referencing authorship)
      (5) Copyright and ownership
      (6) Right to access data (who, when, why)
      (7) Data integrity
         a. Protection of networks, servers, appliances, desktops, laptops, hand held devices and any other electronic device)
         b. Protection of hardware and software
         c. System reliability (viruses, system redundancy, disaster protection)
         b. Inventory and hardware, software, content ownership
      (8) Piracy – see Acceptable Use guidelines
      (9) Hacking – see Acceptable Use guidelines
      (10) Informing and preparing staff and students (compliance with the law)
      (11) Student Safety/Bullying
      (12) FOIP
      (13) Password guidelines and procedures
      (14) Protection of people (identity, reputation) and data (theft, loss, storage and transportation of information)
      (15) Protection of system (reputation) people (identity, reputation) and data (theft, loss, storage and transportation of information)
      (16) What can be in the cloud? On servers? On local computers?
      (17) Cloud computing – know terms of agreement/service, age of consent and age 13 implications, teacher preparedness, account management (right to access – jurisdiction vs teacher creation)
      (18) Privacy rights, responsibilities, and expectations
2. Digital Rights and Responsibilities: Freedoms extended to those in a digital world
   a. Digital Rights and Responsibilities: Acceptable and Responsible Use guidelines Students understand human, cultural, and societal issues related to technology and practice legal and ethical behavior.

(1) Advocate, practice, and teach safe, legal, and responsible use of digital information and technology, including respect for copyright, intellectual property, and the appropriate documentation of sources

(2) Exhibit a positive attitude toward using technology that supports collaboration, learning, and productivity

(3) Demonstrate personal responsibility for lifelong learning

(4) Exhibit leadership for citizenship in a digital age

(5) Sliding scale – Norms of use, consequences if violate norms, communicate and support)

(6) Promote and model digital etiquette and responsible social interactions related to the use of technology and information

(7) Develop and model cultural understanding and global awareness by engaging with colleagues and students of other cultures using digital age communication and collaboration tools

(8) Illicit materials management,

(9) Rights and responsibilities with regard to access to and confiscation

(10) Standards of Conduct – personal nature of online communication)

(11) Accessing communication (e.g. email, cellphone, cloud resources)

(12) Right to access (who can access staff, student communications?)

3. Digital Health and Wellness: Physical and Psychological well-being in a digital world
   a. Ergonomics
   b. Technology Addiction
   c. Balance

Respect and Protect Others: Digital Interactions

1. Digital Communications: Electronic exchange of information
   a. Social Media and Web Based Guidelines and Procedures
      (1) Nature of Privacy and Public Sharing (publicly viewable online content - persistence, searchability, replicability, invisible audiences/strangers)
      (2) Student Safety/Bullying
   b. Students use digital media and environments to communicate and work collaboratively, including at a distance, to support individual learning and contribute to the learning of others.
      (1) Interact, collaborate, and publish with peers, experts, or others employing a variety of digital environments and media
      (2) Communicate information and ideas effectively to multiple audiences using a variety of media and formats
      (3) Develop cultural understanding and global awareness by engaging with learners of other cultures
      (4) Contribute to project teams to produce original works or solve problems
   c. Research and Information Fluency
      Students apply digital tools to gather, evaluate, and use information.
      (1) Plan strategies to guide inquiry
      (2) Locate, organize, analyze, evaluate, synthesize, and ethically use information from a variety of sources and media

        (3) Evaluate and select information sources and digital tools based on the appropriateness to specific tasks
        (4) Process data and report results
    d. Integrity of Identity (digital identity formation/development)
        (1) Support students living one life or two
    e. Student and Staff communication (e.g. cell phones, asynchronous and synchronous mediums)
    f. Personal vs employee/student representation (inappropriate and appropriate public expression)
    g. Content Management (Actively sought and passively received information)
    h. Filtering (sliding scale)
    i. Outside world communication (sliding scale) – see Acceptable Use guidelines
    j. Bring Your Own Device vs. educational value (learning focused environments)

2. Digital Etiquette: Standards of conduct or procedures online
    a. Promote and Model Citizenship in a digital age and Responsibility
    Teachers understand local and global societal issues and responsibilities in an evolving digital culture and exhibit legal and ethical behavior in their professional practices.
    b. Digital Rights and Responsibilities: Acceptable and Responsible Use guidelines
    Students understand human, cultural, and societal issues related to technology and practice legal and ethical behavior.
        (1) Advocate, practice, and teach safe, legal, and responsible use of digital information and technology, including respect for copyright, intellectual property, and the appropriate documentation of sources
        (2) Exhibit a positive attitude toward using technology that supports collaboration, learning, and productivity
        (3) Demonstrate personal responsibility for lifelong learning
        (4) Exhibit leadership for citizenship in a digital age
        (5) Sliding scale – Norms of use, consequences if violate norms, communicate and support)
        (6) Promote and model digital etiquette and responsible social interactions related to the use of technology and information
        (7) Develop and model cultural understanding and global awareness by engaging with colleagues and students of other cultures using digital age communication and collaboration tools
        (8) Illicit materials management,
        (9) Rights and responsibilities with regard to access to and confiscation
        (10) Standards of Conduct – private nature of online communication)
        (11) Accessing communication (e.g. email, cellphone, cloud resources)
        (12) Right to access (who can access staff, student communications?)

3. Digital Access: Full electronic participation in society
    a. Connectivity: wireless and bring your own device guideline and procedures
        (1) Equity of access
        (2) Filtering
        (3) Wireless
        (4) Bring Your Own Device

b. Social Media and Web Based Communication guidelines and procedures

Respect and Protect Intellectual Property and other Property: Digital Preparedness

1. Digital Law: Responsibility for actions and deeds using electronics
    b. Protection of Personal Information Guidelines and Procedures
        (1) Appropriate access
        (2) Risk vs educational and business goals
        (3) Appropriate communication
        (4) Plagiarism, ownership, and responsibility (referencing authorship)
        (5) Copyright and ownership
        (6) Right to access data (who, when, why)
        (7) Data integrity
            a. Protection of networks, servers, appliances, desktops, laptops, hand held devices and any other electronic device)
            b. Protection of hardware and software
            c. System reliability (viruses, system redundancy, disaster protection)
            c. Inventory and hardware, software, content ownership
        (8) Piracy – see Acceptable Use guidelines
        (9) Hacking – see Acceptable Use guidelines
        (10) Informing and preparing staff and students (compliance with the law)
        (11) Student Safety/Bullying
        (12) FOIP
        (13) Password guidelines and procedures
        (14) Protection of people (identity, reputation) and data (theft, loss, storage and transportation of information)
        (15) Protection of system (reputation) people (identity, reputation) and data (theft, loss, storage and transportation of information)
        (16) What can be in the cloud? On servers? On local computers?
        (17) Cloud computing – know terms of agreement/service, age of consent and age 13 implications, teacher preparedness, account management (right to access – jurisdiction vs. teacher creation)
        (18) Privacy rights, responsibilities, and expectations
2. Digital Literacy: Process of teaching and learning about technology and the use of technology
    a. Expectations for students and staff to develop digital literacy. Infusion of technology and modeling of digital age work and learning. Teachers exhibit knowledge, skills, and work processes representative of an innovative professional in a global and digital society.
    b. Digital Rights and Responsibilities: Acceptable and Responsible Use guidelines Students understand human, cultural, and societal issues related to technology and practice legal and ethical behavior.
        (1) Advocate, practice, and teach safe, legal, and responsible use of digital information and technology, including respect for copyright, intellectual property, and the appropriate documentation of sources
        (2) Exhibit a positive attitude toward using technology that supports collaboration, learning, and productivity

- (3) Demonstrate personal responsibility for lifelong learning
- (4) Exhibit leadership for citizenship in a digital age
- (5) Sliding scale – Norms of use, consequences if violate norms, communicate and support)
- (6) Promote and model digital etiquette and responsible social interactions related to the use of technology and information
- (7) Develop and model cultural understanding and global awareness by engaging with colleagues and students of other cultures using digital age communication and collaboration tools
- (8) Illicit materials management,
- (9) Rights and responsibilities with regard to access to and confiscation
- (10) Standards of Conduct – private nature of online communication)
- (11) Accessing communication (e.g. email, cellphone, cloud resources)
- (12) Right to access (who can access staff, student communications?)

- c. Standard operating procedures
  - (1) Demonstrate fluency in technology systems and the transfer of current knowledge to new technologies and situations
  - (2) Collaborate with students, peers, parents, and community members using digital tools and resources to support student success and innovation
  - (3) Communicate relevant information and ideas effectively to students, parents, and peers using a variety of digital age media and formats
  - (4) Model and facilitate effective use of current and emerging digital tools to locate, analyze, evaluate, and use information resources to support research and learning

3. Digital Commerce: Online buying and selling of goods
   - a. Preparation for online transactions

ATTACHMENT #2

Horizon School Division # 67
DIGITAL RIGHTS AND RESPONSIBILITIES
ACCEPTABLE AND RESPONSIBLE USE
ADMINISTRATIVE GUIDELINES

DEFINITIONS

ELECTRONIC TECHNOLOGY RESOURCES

ELECTRONIC TECHNOLOGY RESOURCES REFERS TO ALL RESOURCES ON AND OFF THE NETWORK OF HORIZON SCHOOL DIVISION INCLUDING BUT NOT LIMITED TO: ALL HARDWARE, SOFTWARE, SERVICES (SUCH AS E-MAIL AND INTERNET ACCESS) AND INFORMATION RESOURCES (SUCH AS PERSONAL FILE STORAGE)].

GUIDELINES

1. Jurisdictional electronic technology resources are intended for educational purposes and for business activities in the operation of schools and the division.

2. The use of electronic technology resources is subject to all policies and practices of both the division and the school. Divisional policy shall supersede school policy.

3. Staff who deliberately use jurisdictional electronic technology resources inappropriately will be subject to disciplinary or legal action, which may include termination of employment.

4. The division has the right to supervise the use of electronic technology resources. All users of such property should expect only limited privacy in the contents of any personal files or record of web research activities on the network. Horizon reserves the right to monitor, log, and search any and all aspects of its computer system and network including e-mail communications when required for operational needs or where there are reasonable grounds to suspect abuse, misuse, or noncompliance with Horizon School Division policies, regulations, administrative guidelines, or improper or illegal activity.

5. The jurisdiction has the right to specify who uses its electronic technology resources and the information contained therein, under what circumstances and to what purpose. Equipment purchased by the division belongs only to the division and neither employees, volunteers, nor students in the division have ownership rights to any equipment loaned to them by the division.

6. Any violation of this policy may result in, but not limited to:

   a. Loss of access privileges

   b. Loss of volunteer position

   c. Student discipline measures

   d. Employee discipline action such as employment suspension or termination or

   e. Legal action, including criminal prosecution

7. All students should have the opportunity within available resources to access electronic technology resources to enhance learning.

8. The school has the responsibility to effectively manage and utilize electronic technology resources in order to maximize student learning opportunities.

9. Central coordination of computer resources is essential to the development and maintenance of an effective computer network.

10. Personal electronic technology resources such as cell phones, laptops, PDAs, digital music players, and other one way and two way communication devices that users may have access to or bring from home are dealt with under COMMUNICATION: SOCIAL MEDIA, WEB BASED AND DIVISION-OWNED VECHILES (Attachment #4) ADMINISTRATIVE GUIDELINES.

11. Access to electronic technology resources is a privilege, not a right and users are expected to demonstrate the same kind of responsible behaviour while working or communicating in an electronic environment as would be expected of them in a classroom and/or school face to face setting.

    11.1 When issues arise schools will utilize them as citizenship learning opportunities

PROCEDURES

1.0 Users

1.1 Users shall not be granted access to the jurisdictional network including Internet access until network agreements are signed. Such users are expected to adhere to citizenship in a digital age standards.

2.0 Schools

2.1 Given Horizon's membership in the Southern Alberta Computer Consortium and its computer acquisition agreement, schools shall coordinate all electronic technology purchases with the technology department to ensure alignment with the SACC agreement.

2.2 Schools are responsible for ensuring staff are able to effective utilize available electronic technology.

2.3 School principals shall be responsible for having school procedures in place that provide opportunity for student access to electronic technology resources including signed acceptable use agreements for all students accessing the network. These procedures shall also address consequences of inappropriate behaviour.

2.3.1 School staff shall ensure that all students receive Citizenship in a digital age and network training with particular attention being given to procedures, responsible use, and security before allowing them to use the network.

3.0 School Division

3.1 Hardware/software acquisition planning shall reflect student program objectives and hardware selection will be based on the most effective solution for the program area.

3.2 The technology department in consultation with the administrator group shall be responsible for blocking Internet sites that are deemed to be inappropriate for users.

3.2.1 Filtering of Internet sites will provide flexibility given the unique cultural contexts. School Principals may request to the office of the Superintendent that sites and categories be removed from being blocked on a permanent or temporary basis when access to the information contained on the site is deemed appropriate.

3.3 Horizon School Division network storage areas and email provided to individual users are not private property. Horizon School Division network administrators may review files and communications to maintain system integrity and ensure the system is being used in a responsible manner.

3.4 Horizon School Division shall have in place policy and procedures that outline the contractual arrangements for users of electronic technology resources. The contracts shall specify terms and conditions of use, prohibited activities and consequences for breaking the agreement and be signed by or digitally accepted by the staff, or user.

4.0 Software

4.1 Only division or school owned software programs will be installed on Horizon School Division computer equipment.

4.2 Software installation will normally be done in consultation with the certified technical staff of the Horizon School Division and carried out in a manner consistent with established practices.

4.3 Software in use will be utilized only within the framework of purchase or license and copyright agreements.

5.0 Internet

5.1 All users shall adhere to division responsible use guidelines.

6.0 Liability

The Horizon School Division assumes no responsibility or liability if documents stored on Division equipment are lost or damaged, nor will the Division be responsible for security violations beyond the appropriate response to those persons involved in such violations. While the jurisdiction provides a level of redundancy of information, users are responsible for making backup copies of the documents critical to themselves.

STUDENT CONTRACT FOR THE RESPONSIBLE USE OF ELECTRONIC TECHNOLOGY RESOURCES AND COMPUTER NETWORKS

Throughout this document **"Horizon School Division"** is used to represent the Board of Trustees of Horizon School Division.

The Horizon School Division believes in the use of technology to develop the competencies they will need to be successful in life. Technology supports the teaching and learning environment and engages and empowers the learning community. The jurisdiction further recognizes that citizenship in a digital age is fundamental to the provision of citizenship and quality education within such learning environments.

In consideration of ________________________________ being granted access to the wired and wireless network, including the issuance of a personal account for use on the system, the parties, including the student, his or her parent(s) or legal guardian(s), the sponsoring teacher, and the Board acknowledge and agree as follows:

1. Privileges

The use of the Internet is a privilege, not a right, and inappropriate use (as determined by Horizon School Division Staff) will result in a cancellation of those privileges.

2. Supervision

The division has the right to supervise the use of electronic technology resources. All users of such property should expect only limited privacy in the contents of any personal files or record of web research activities on the network. Horizon reserves the right to monitor, log, and search any and all aspects of its computer system and network usage including e-mail communications when required for operational needs or where there are reasonable grounds to suspect abuse, misuse, or noncompliance with Horizon School Division policies and regulations or improper or illegal activity.

3. Responsible Use

This Responsible Use Agreement is required for student use of any digital device in any Horizon School Division school. The Agreement will remain in effect until revoked by parents or administration. Contracts may be reviewed each school year as a springboard for teaching and learning around topics such as Internet safety, citizenship in a digital age and ethical use of technology.

Respecting and abiding by Canadian law, whether Federal, Provincial, Municipal or other statute, Transmission of any material in violation of any Federal or Provincial regulation is prohibited. This includes but is not limited to the following:

Students will not engage in:

(a) Illegal or unethical acts, including attempts to damage or destroy computer based information or information sources, involvement in plans to defraud, and downloading or transmission of unlawful information.
(b) Downloading or transmission of pornographic, obscene or other socially unacceptable materials including profanity; vulgarities; sexual, racial, religious, or ethnic slurs
(c) Gaining access to or revealing the personal data of others without authorization
(d) Installation or transfer of commercial software, materials protected by trade secret or other copyright protected material where a registration fee is required by the author.

(e) Sending messages or files containing any form of electronic information that is likely to result in loss or disruption of the recipient's work or system.

(f) Plagiarism of information obtained via Internet.

I agree to the following:

Respect and Protect Yourself: Digital Well-being

- Use only my own personal login and keep my password private.
- Keep my personal information private. Do not give out personal information (address, telephone number, parents' work address/telephone number, or name and location of your school) without parental or teacher permission.
- Select online names that are appropriate.
- Not publishing my personal details, contact details or a schedule of my activity where strangers have access.
- Not revealing my passwords to anyone except Horizon employees.
- Use technology/Internet only with permission.
- Talk to a teacher if I feel uncomfortable or unsafe online or see others participating in unsafe, inappropriate or hurtful online behavior.
- Seek to understand the terms and conditions of websites and online communities.
- Tell an adult if you come across any information that makes you feel uncomfortable.
- Never agree to get together with someone you "meet" on-line without parental consent.
- Never send a personal picture or anything else without parents or teacher consent.
- That content I upload or post becomes part of my digital footprint, a foot print I will keep appropriate.
- Guide my use of technology and judge appropriateness of communication (text and image) knowing that it is permanent and can be accessed by someone years later.

Respect and Protect Others: Digital Interactions

- Protect privacy rights including not giving out my or others' personal details including full names, telephone numbers, addresses and images.
- Refrain from using profanity or abusive language.
- Refrain from actions that are malicious or harmful to others.
- Not use technology to bully or tease other people.
- Protect others by reporting abuse and not forwarding inappropriate materials or communications.
- Treat others with dignity and respect.
- Refrain from sharing information about others without their knowledge or consent.
- Refrain from posting or storing content that contains sexual, racial, religious, or ethnic slurs, any other form of abuse, or that contain threatening or otherwise offensive language or pictures.
- Respect the privacy of others.
- Not interfere with network security, the data of another user or attempt to log into the network with a user name or password of another student.

Respect and Protect Intellectual Property and other Property: Digital Preparedness

- Suitably cite any and all use of websites, books, media etc.
- Request to use the software and media others produce.
- Use all technology resources in school responsibly, respecting the learning environment.
- Abide by copyright procedures when using content on websites (ask permission to use images, text, audio and video and cite references where necessary).

I also agree to:

- Use digital devices in school to enhance learning across the curriculum.
- Demonstrate citizenship in a digital age in all online communication, including social networking.
- Respect the laws or rules of any other state, international agency or organization with whom I interact,
- Ensure I am authorized to access resources either inside or outside of the network prior to accessing them,
- Be a safe, responsible and ethical user whenever and wherever I use technology
- Use the internet for educational purposes and only as directed by Horizon staff

4. **Liabilities**
   Horizon School Division makes no warranties of any kind, whether expressed or implied, for the service it is providing. Horizon School Division will not be responsible for any damages or losses of data you suffer. Use of the Internet is at your own risk. Horizon School Division specifically denies any responsibility for the accuracy of or quality of information obtained through this service.

5. **Security**
   Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem in the system, you should notify a teacher or system administrator. Do NOT demonstrate network problems to other users.

   Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network. I, the undersigned, understand and will abide by the above **Terms and Conditions** for the Internet and network use. I further understand that violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation my access privileges may be revoked, school disciplinary action and/or appropriate legal action may be taken.

In addition, we ask that parents and students sign below to agree to the following terms and conditions, which are specific to using personal devices.

When I use my own wireless device (phone, iPod, iPad, laptop, or other wireless device) I agree to:

a. only bring my wireless device into the classroom when approved by a teacher, and leave it on silent mode and in full view at all times.

b. be responsible for the device at all times. It is my responsibility to ensure that it is locked in my locker at all times when not specifically required in the classroom.

c. protect the privacy of others and never post or forward personal information about another person using Short Message Service (SMS)

d. only take photos and record sound or video when it is part of an approved lesson

e. seek verbal permission from individuals involved before taking photos, recording sound or videoing them (including teachers)

f. seek written permission from individuals involved before uploading or sending photos, recorded sound or video to anyone else or to any online space

g. be respectful in the photos I take or video I capture and never use these as a tool for bullying.

This Acceptable Use Agreement also applies during school excursions, camps and extra-curricular activities. I acknowledge and agree to follow these rules. I understand that my access to the internet and wireless technology at school will be renegotiated or revoked if I do not act responsibly.
Please sign and return the attached page to the school.

I, the undersigned, understand and will abide by the above **Terms and Conditions** for the Internet and network use. I further understand that violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation my access privileges may be revoked, school disciplinary action and/or appropriate legal action may be taken.

Student Signature: ________________________ Date: __________________________
Parent Signature: _________________________ Date: __________________________

STAFF/ADULT USER CONTRACT FOR THE AGREEMENT OF DIVISION COMPUTERS AND COMPUTER NETWORKS

Staff/Adult Name: ________________________________

Staff/Adult Acceptable Use Agreement

Horizon School Division believes in the use of technology to develop the competencies students need to be contributing global citizens and for the creation of student-centred learning environments. Users are provided access to Horizon's G Suite Domain (Google Apps for Education), the digital network, and a variety of devices and services.

Throughout this document **"Horizon School Division"** is used to represent the Board of Trustees of Horizon School Division.

1. **Privileges**
   Staff who deliberately use jurisdictional technology inappropriately will be subject to disciplinary or legal action, which may include termination of employment. Appropriate personal use of technology is permitted provided the use does not interfere with the user's work performance, interfere with any other user's performance, have undue impact on the operation of the network or violate any policy, guideline or standard of Horizon School Division.

2. **Supervision**
   The division has the right to supervise the use of electronic technology resources. All users of such property should expect only limited privacy in the contents of any personal files or record of web research activities on the network. Horizon reserves the right to monitor, log, and search any and all aspects of its digital environment including e-mail communications when required for operational needs or where there are reasonable grounds to suspect abuse, misuse, or noncompliance with Horizon School Division policies and regulations or improper or illegal activity.

3. **Acceptable Use**
   The use of your account and the division's devices/network must be in support of education and research and consistent with the educational objectives of the Horizon School Division. Transmission of any material in violation of any Federal or Provincial regulation is prohibited. This includes but is not limited to the following:

   Staff/Adult user will not engage in:

   (a) Illegal or unethical acts, including attempts to damage or destroy computer based information or information sources, involvement in plans to defraud, and downloading or transmission of unlawful information.
   (b) Downloading or transmission of pornographic, obscene or other socially unacceptable materials including profanity; vulgarities; sexual, racial, religious, or ethnic slurs
   (c) Gaining access to or revealing the personal data of others without authorization
   (d) Installation or transfer of commercial software, materials protected by trade secret or other copyright protected material where a registration fee is required by the author.
   (e) Sending messages or files containing any form of electronic information that is likely to result in loss or disruption of the recipient's work or system.
   (f) Activities that are wasteful of, degrade, or disrupt network resources or performance
   (g) Theft of time activities: online activities not in alignment with roles, responsibilities, and or duties
   (h) On-line gambling services.
   (i) Business or financial transactions for personal financial gain
   (j) Accessing, collecting, using, or disclosing information they do not need for their duties

CRIMINAL AND CIVIL LAW IMPLICATIONS

Inappropriate use of electronic communication and social media can also result in an employee being criminally charged and convicted or facing civil action. Examples of actions and resulting charges are:

- making inappropriate online comments that lead to civil actions, such as defamation
- disclosing confidential information about the school, students and colleagues, thus breaching workplace privacy policies and provisions of the School Act
- posting the work of others without proper attribution, raising copyright-violation issues
- breaching a court-ordered publication ban
- inciting hatred against an identifiable group
- disclosing information about a minor, contrary to the Youth Criminal Justice Act
- using technology to harass a student, colleague or others, contrary to the Criminal Code
- using a computer to lure a child or for juvenile prostitution under the Criminal Code
- exchanging or forwarding compromising photos, videos or audio recordings of students leading to charges of possession or distribution

Electronic communication and social media can also be used as evidence in criminal and civil proceedings.

4. **Responsible Use**

The Horizon School Division provides ongoing student instruction that develops citizenship in a digital age over time. Technology also complements teaching and learning as outlined in Alberta Education's Learning and Technology Policy Framework and the Ministerial Order on Student Learning (#001/2013).

Respect and Protect Yourself: Digital Well-being

A. Staff demonstrate a sound understanding of technology concepts, systems, and operations.
   - I will understand, select, and use technology systems and application purposefully.
   - I will transfer current knowledge to learning of new technologies.

B. Staff employ strategies to protect personal security and identity.
   - I will protect personal username and password information.
   - I will protect all data related to personal identity.
   - I will protect personal reputation in all digital interactions.
   - I will self-monitor appropriate access and use of digital assets.

C. Staff model digital well-being in the course of all actions.

Respect and Protect Others: Digital Interactions

A. Staff understand human, cultural and societal issues related to technology and practice legal, ethical behaviour.
   - I will promote and model digital etiquette and responsible social interactions related to the use of technology and information.
   - I will develop and model cultural understanding and global awareness by engaging with colleagues and students of other cultures using digital age communication and collaboration tools.

B. Staff exhibit knowledge, skills, and work processes representative of an innovative professional in a global and digital society.
   - I will demonstrate fluency in technology systems and the transfer of current knowledge to new technologies and situations.
   - I will collaborate with students, peers, parents, and community members using digital tools and resources to support student success and innovation.
   - I will communicate relevant information and ideas effectively to students, parents, and peers using a variety of digital age media and formats.

- I will model and facilitate effective use of current and emerging digital tools to locate, analyze, evaluate and use information resources to support research and learning.

C. Staff ensure a welcoming, caring, respectful and safe learning environment free from bullying and harassment.

- I will ensure all students comply with expectations for a welcoming, caring, respectful and safe learning environment in all digital interactions and uses of technology.

D. Staff conduct all digital interactions and uses of technology in a manner reflective of the values of the school and the school division.

Respect and Protect Intellectual Property and Other Types of Property: Digital Preparedness

A. Staff demonstrate responsibility for safety and security of technology, including data, software, and hardware.

- I will teach and model safe, legal and responsible use of technologies, including understanding and compliance with Terms of Service agreements.
- I will demonstrate safe and responsible use of networks, servers, computers and devices.
- I will immediately report any detection of malware or threat of ransomware to the technology department.

B. Staff follow legal and ethical guidelines for attribution of all sources to avoid plagiarism of content or images.

C. Staff follow legal guidelines for all copyright materials.

5. Warranties

The Horizon School Division makes no warranties of any kind, whether expressed or implied, for the service it is providing. Horizon School Division will not be responsible for any damages or losses of data or property a user may suffer. Use of the internet is at your own risk. Horizon School Division specifically denies any responsibility for the accuracy of or quality of information obtained through this service.

6. Earnings and T4 Statements

As an employee of Horizon School Division I recognize and agree to the electronic distribution of earnings and T4 statements. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

I, the undersigned, understand and will abide by the above **Terms and Conditions** for the Internet and network use. I further understand that violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation my access privileges may be revoked, school disciplinary action including dismissal and/or appropriate legal action may be taken.

______________________________ ______________________________ ________________

NAME (PLEASE PRINT) SIGNATURE DATE

ATTACHMENT #3

Horizon School Division # 67

PROTECTION OF PERSONAL INFORMATION ADMINISTRATIVE GUIDELINES

INTRODUCTION

Section 38 of the FOIP Act requires a public body to protect sensitive and confidential information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction. These guidelines and procedures address Horizon's privacy obligations regarding the protection of personal information and specifically the security of digital data on portable computing devices (e.g. laptop computers) and portable storage devices (e.g. USB sticks), and web based applications. Furthermore, it makes specific recommendations to reduce such risks.

Practices within Horizon School Division regularly include the collection of confidential student information (e.g. student names, addresses, phone numbers, grades, etc), which are backed up (in some cases off-site) to comply with data redundancy and disaster recovery guidelines. Teachers and especially administrators and counselors regularly store sensitive information on personal USB sticks or utilize the synchronization utility on their laptops to transfer data between servers and local hard drives. When these devices are then transported off site, data is at risk of a privacy breach should the device be lost or stolen.

Computing devices, such as laptops, as well as storage media, such as CDs, DVDs, and USB drives, all have the potential of falling into the wrong hands, particularly when they are not stored in a secure location. The highly publicized case in England where 25 million people's sensitive and confidential information was compromised as well as other high-profile privacy rulings relating to the inappropriate disclosure by a public body of sensitive and confidential information located on lost or stolen portable storage devices (e.g. USB sticks and laptop computers) has compounded the need to address this issue. In these rulings, the courts found that loss and theft of portable computing and storage devices are well known and publicized, making the risk real and foreseeable. Password protection while an essential part of a data security plan is not adequate protection by itself.

DEFINITIONS:

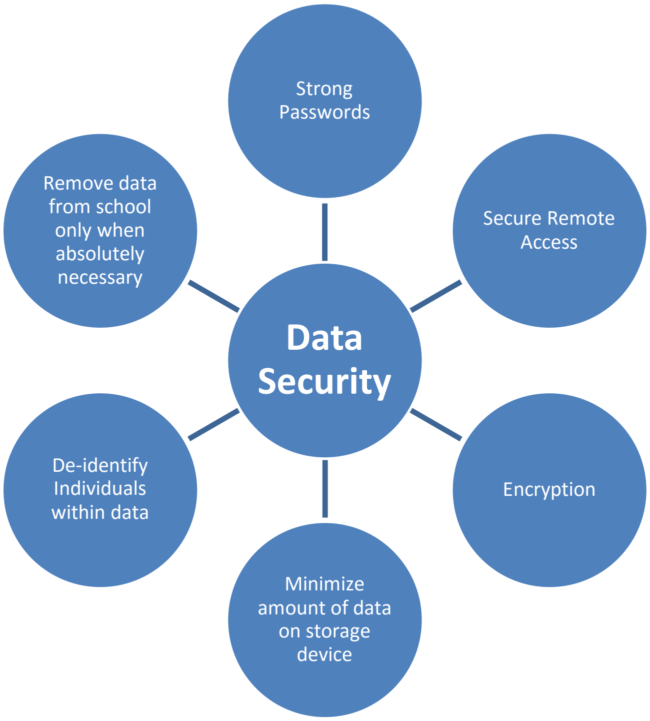
The term personal information is a critical element within the FOIP Act. The definition according to the Act follows:

Personal Information means recorded information about an identifiable individual, including

(a) the individual's name, home or business address or home or business telephone number,
(b) the individual's race, national or ethnic origin, colour or religious or political beliefs or associations,
(c) the individual's age, sex, marital status or family status,
(d) an identifying number, symbol or other particular assigned to the individual,
(e) the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics,
(f) information about the individual's health and health care history, including information about a physical or mental disability,
(g) information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given,
(h) anyone else's opinions about the individual, and

(i) the individual's personal views or opinions, except if they are about someone else; (Alberta Queen's Printer, 2009)

Protecting personal information consists of six key activities (shown in the schematic and described in more detail below).


Strong Passwords
Remove data from school only when absolutely necessary
Secure Remote Access
Data Security
De-identify Individuals within data
Encryption
Minimize amount of data on storage device

Encryption: Any procedure used in cryptography to convert plain-text into cipher-text in order to prevent anyone except the intended recipient from reading that data. There are many types of data encryption, and they are the basis of network security.

Encryption Key: A sequence of characters used by an encryption algorithm to encrypt plain-text into cipher-text.

Key Management: In cryptography, keys are required for decipherment and authentication. These procedures provide no security when the keys have been handled incorrectly. Key management implies the effective creation, storage, transmission, installation and eventual destruction of keys

Https: The protocol for accessing a secure Web server. Using HTTPS in the URL instead of HTTP directs the message to a secure port number rather than the default Web port. The session is then managed by a security protocol.

Secure Remote Access (VPN): A virtual private network (VPN) is a private data network that makes use of public infrastructure, maintaining privacy through the use of a tunnel protocol and security procedures.

GUIDELINES

1. The Board of Trustees shall designate the Superintendent of Schools as Head for Horizon School Division. The Head is responsible and accountable for all decisions taken under the FOIP Act and has the authority to delegate duties to comply with this Act.

2. The Board of Trustees shall designate the Secretary-Treasurer as Coordinator for Horizon School Division. The FOIP Coordinator will perform the administrative duties required within this Act for Horizon School Division's operations.

3. Students, parents, Horizon School Division employees, independent service contractors, and vendors provide personal information to Horizon School Division with the understanding that the Division will use the information only as necessary to carry out the Division's mandate

4. All information must be maintained in confidence and disclosed only if authorized by regulation or law including, but not limited to, the School Act, the Freedom of Information and Protection of Privacy Act, the Child Welfare Act, and the Income Tax Act.
    a. All digital images and recordings of an individual at school during the course of regular school day activities become a collection of personal information and therefore must comply with the Freedom of Information and Protection of Privacy (FOIP) Act.
    b. At events open to the public, Horizon School Division cannot be reasonably expected to limit the recording and distribution of personal images.
    c. While at school and school sponsored functions, with the exception of independent students, parents must grant permission prior to the dissemination of student images and confidential information beyond the secure school or network environment of Horizon School Division.
        i. At the time a student registers at a school in Horizon School Division, the parent of the student shall be provided with the opportunity to give written consent for the publication of the student's name and photograph in school related activities and operation while a student in the Division.
    d. Only authorized persons may use, disclose, take, alter, copy, interfere with, or destroy information, and must do so according to law and Horizon School guidelines, procedures, and practices.

5. Records management guidelines shall be followed by schools and Division departments.

DATA STORAGE GUIDLINES

1. All records created by Horizon School Division employees in the course of their work are subject to the Freedom of Information and Protection of Privacy Act and are under the custody and control of the Division at all times.

   a. The Freedom of Information and Protection of Privacy Act and the orders provided by the privacy commissioner set the standards for the security of personal information. The Board will administer the Freedom of Information and Protection of Privacy Act as legislated by the Province of Alberta.

2. The security of information has the potential of being compromised when the information is stored on portable devices, personal information devices or when the information is transported to and from the worksite.

   a. Each person using confidential information is responsible for the management and safekeeping of information under their control by ensuring that there is adequate security to prevent unauthorized access, collection, use, disclosure or disposal of information.

   b. Each employee is to ensure the risk of unauthorized disclosure of personal or other confidential information is minimized. Records that are maintained in digital format must comply with guidelines delineated in this document.

   c. The FOIP Act requires protection of personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction. School principals shall ensure that an adequate level of security is provided for all personal information that is in their control and custody and shall ensure that the staff they supervise are aware of their responsibility as outlined in the attachments within this policy.

      - Confidential **data should be retained and removed from schools only when necessary**.

      - When retention is required, **data should be password protected and encrypted whenever it is stored in locations that are not physically secured with physical and technical access controls appropriate to the sensitivity of the data**.

         - The purpose of encryption is to prevent unauthorized access to confidential or sensitive information while it is either in storage or being transmitted.

         - In order to accomplish this, proper key management is crucial. If a key gets into the wrong hands, unauthorized access to information can result. Conversely, if a key is lost or destroyed, critical information may become unavailable to authorized personnel. Care should be taken to ensure the integrity of the key repository. This repository is confidential data in itself, so strong protections and access control, must be implemented. Encryption is not, however, a panacea. It is not a substitute for other security measures, such as authentication, authorization, and access control, and must be used in conjunction with other measures including:

- Keeping the **amount of** sensitive and confidential **information** stored **on** mobile computing and storage **devices to a minimum**, based on need;
- De-identification of sensitive and confidential information if possible (e.g. removal of identifying characteristics such as name);
- **Not using the synchronization process, or if utilized, configuring the process so that only a limited number of files are transferred**, containing current works in progress, thereby reducing the amount of information on laptops to essential data;
- **Protection of files and folders by not sharing logon passwords** and in the case of cloud storage (e.g. Dropbox, Google drive), not sharing account usernames and or passwords.
- Ensuring that the portable device is **labeled with appropriate contact information** in the case of loss;
- Ensure portable storage devices are **not left in non-secured areas**.

ENCRYPTION

Microsoft Windows includes the ability to encrypt data directly on volumes that use the NTFS file system so that no other user can use the data. You can encrypt files and folders if you set an attribute in the object's **Properties** dialog box.

USB sticks can also be purchased containing vaults which can store encrypted data.

1. How files are encrypted

   a. Files are encrypted through the use of algorithms that essentially rearrange, scramble, and encode the data. A key pair is randomly generated when you encrypt your first file. This key pair is made up of a private and a public key. The key pair is used to encode and decode the encrypted files.

   b. If the key pair is lost or damaged and you have not designated a recovery agent then there is no way to recover the data.

2. How to encrypt a folder

   a. Although you can encrypt files individually, generally it is a good idea to designate a specific folder where you will store your encrypted files, and to encrypt that folder. If you do this, all files that are created in or moved to this folder will automatically obtain the encrypted attribute.

   i. Locate and right-click the folder that you want, and then click **Properties**.
   ii. On the **General** tab, click **Advanced**.
   iii. Click the **Encrypt contents to secure data** check box, and then click **OK**.
   iv. In the **Confirm Attribute Changes** dialog box that appears, use one of the following steps:
      - If you want to encrypt only the folder, click **Apply changes to this folder only**, and then click **OK**.
      - If you want to encrypt the existing folder contents along with the folder, click **Apply changes to this folder, subfolders and files**, and then click **OK**.

b. The folder becomes an encrypted folder. You will know if files are encrypted as they will appear green. Note that this does not prevent others from viewing the contents of the folder. This prevents others from opening items in the encrypted folder.

3. How to encrypt a USB stick

a. Although you can encrypt files individually, generally it is a good idea to designate a specific folder where you will store your encrypted files, and to encrypt that folder. If you do this, all files that are created in or moved to this folder will automatically obtain the encrypted attribute.

b. **NOTE**: You can encrypt files and folders only on volumes that use the NTFS file system. Since USB sticks typically are formatted as FAT or FAT32 the first thing to do is reformat them to NTFS.
   i. Right-click **USB drive** [e.g. Kingston (E:)] and click on **Format**.
   ii. Locate **File System** and change from **FAT to NTFS**, click **OK**
   iii. You can now create and encrypt folders on the USB device similar to folders. (See “How to encrypt a folder” above for details.)

c. Note: the encrypted USB stick as done above will only allow that USB stick to be used on computers that are logged in with your username and password. If you go to a different computer (e.g. your home computer and log one with a different account you may not be able to open the USB stick. To encrypt a USB and allow it to open on multiple computers you may need to purchase USB sticks that have encryption built into them.

4. How to encrypt data within Dropbox

a. While third party cloud storage providers such as Dropbox encrypt data there have been data breaches reported in the past. To mitigate the likelihood of confidential data being accessed when entrusted in third party data storage solutions it is strongly encouraged to:

i. Limit the extent of confidential data stored in the cloud
ii. When stored provide a second level of encryption under the control of the owner of the data. Third party products such as Secretcrypt (https://getsecretsync.com/ss/) will encrypt data prior to being placed and synced via Dropbox.

5. Encryption of data within other service providers
   a. Staff storing confidential data on external service providers hardware should be cognizant of the level of encryption provided.
   b. Google drive for instance is the same level of encryption as gmail.
   c. Sites lacking adequate levels of encryption should not be utilized to store confidential data

STRONG PASSWORDS

"PASI" means the Provincial Approach to Student Information and entails an application maintained by Alberta Education. PASI is jointly controlled by multiple parties and all users who have access to PASI have access to Alberta students' confidential information. As such, all parties require a common understanding around the protection of this confidential information.

PASI requires Horizon to enter into a "PASI Acceptable Usage Agreement" which requires us to have an "Information Security Guidelines" which addresses the need for the protection of personal information.

To comply with the provincial "PASI Acceptable Usage Agreement" all those Horizon employees whom have access to personal information as defined under FOIP are required to implement physical and technical safeguards for all workstations that access electronic protected information.

Jurisdictions will implement physical and technical safeguards for all workstations that access electronic protected information. Appropriate measures should include:

- Restricting physical access to workstations to only authorized personnel. Securing workstation (Ctrl-Alt-Del and click on lock) prior to leaving area to prevent unauthorized access.
- Enabling password protected screen savers with short timeout periods (15 minutes) to ensure unattended workstations will be protected

Passwords are a means of controlling access to information. Unauthorized access can compromise information confidentiality, integrity and availability resulting in liability, loss of trust or embarrassment to Horizon School Division. Staff are expected to use strong passwords and ensure password confidentiality and protect the data within the Horizon School Division Network.

Strong Password: A strong password is constructed so that another user or a "hacker" program cannot easily guess it. It is typically a minimum number of characters in length and contains a combination of alphabetic, numeric, or special characters. Combine short, unrelated words with numbers, special characters, or mixed case. For example: eAt42peN

Password requirements:

All passwords, including initial passwords, must be constructed, implemented, and maintained according to the Horizon School Division password guidelines. Password guidelines vary dependent on the User within the Horizon School Division Network.

All passwords must

- Be treated as confidential information (Are never shared except with admin or tech support when required)
- Be changed immediately if the security of the password is in doubt (compromised or you are aware others know it)
- Be encrypted when stored or transmitted.
- Contain both upper and lower case characters (i.e. a-z, A-Z) as outlined in the table below
- Have digits as well as letters (i.e. 0-9) as outlined in the table below
- Are at least 5 alphanumeric characters long
- Not be written down in an unsecured locaton
- Never be shared, and when protecting confidential information should be unique to that account (do NOT use a generic password that is used for nonwork purposes).

Those with access to highly confidential information (school secretaries, principals, and counselors) are encouraged to change their passwords on a regular bases (etc yearly)

Passwords should not be easily related to such personal information as:

- Your logon Name or employee ID
- Your nickname
- Your social security or driver's license number
- Your birthday
- Word or number patterns such as aaabbb, zyxwvut, 123321, etc.
- Obscenities
- School names, school mascot, or school slogans
- Being the same as other passwords selected for personal use outside of the office, or passwords commonly used on public web sites.

The following chart specifies the password complexity requirements for different users' accounts:

	Minimum Length	Complex Password	Minimum Alpha Characters (Letters)	Minimum Upper Case Alpha Characters (Letters)	Minimum Digits (Numbers)	Minimum Special Characters
System Accounts	8	Yes	1	1	2	1
Senior Admin Staff and Trustees	8	Yes	1	1	1	0
Administrators, Admin Support Staff, and Teaching Staff	8	Yes	1	1	1	0
Other Staff	8	Yes	1	0	1	0
K-6 Students	5	No	1	0	0	0
6-12 Students	8	Yes	1	0	1	0

Constructing a Strong Password

To construct a strong password staff and gr. 7-12 students must use the first three of the following character sets and have a minimum of 10 characters:

- Upper case alpha characters/letters (A – Z)
- Lower case alpha characters/letters (a – z)
- Numbers (0-9)
- Special Characters (#$%&* etc.)

It is recommended that one think of using pass phrases as opposed to passwords. Here are some examples of what constitutes a complex password:

1L0veh0r1zoN!   Myd0giSwh1te   Gre@tnew5!

Application Password Information

The application environment within the Horizon School Division consists of applications that authenticate to Active Directory and some that use different authentication methods that are dependent on what the particular technology allows.

In most cases, the password does not display while it is being entered. Applications hosted on the jurisdiction network have not been written to enforce a strong password. Now that password standards have been defined, the long term plan is to configure applications to authenticate against Active Directory, and to enforced password guidelines through those services.

This is a more efficient and reliable means of ensuring consistency in standards than having each application enforce standards independently. Currently applications that do not support active

directory authentication must comply with existing policies and need to be enforced by the department identified as responsible for the system(s) in question.
Staff's Signature

PASSWORD PROTECTED SCREEN SAVER

Must be employed by: Senior Administrative Leadership Team, School Administration, SIS operators, and Classroom Support Teachers. This is essential for mobile devices which provide access to confidential information via email.

Windows XP

- Right Click – chose “properties” from menu
- Click “Screen Saver” tab – found along the top
- Click the down arrow and chose the screen saver you want
- Check the box “on resume, display logon screen”
- Set the time for screen saver to come on – maximum time of 30 minutes

Windows 7

- Right Click – chose “personalize” from menu
- Click “Screen Saver” – found in bottom right corner
- Click the down arrow and chose the screen saver you want
- Check the box “on resume, display logon screen”
- Set the time for screen saver to come on – maximum time of 30 minutes

IPhone Password

- Click “settings”
- Click “general”
    - Set auto-lock to 5 or less minutes
    - Turn “passcode lock” on

DATA ACCESS GUIDELINES

1. The right to access information and the protection of privacy shall be managed in compliance with the FOIP Act.

    a. A fee shall be assessed prior to processing a FOIP application for general records.

    b. Fees for a FOIP applicant requesting his/her own personal information shall be restricted to the cost of providing a copy of the information.

2. Network access is controlled through the use of login passwords. Because such passwords provide access to staff domains and sensitive and confidential student information such **passwords should be considered confidential**, even when no confidential data is being accessed or transmitted. Many technology department login passwords provide greater access to Horizon’s network and should also be considered confidential.

3. Computing devices containing or having access to sensitive and confidential information should be protected with **strong login passwords** (see Appendix C) and utilize further security features such as **password protected screen savers** (see Appendix D).

DATA TRANSMISSION GUIDELINES

1. Schools should ensure appropriate security protocols are in place whenever confidential data is removed or accessed off site. This includes **encryption** of confidential data but should also include a **determination on whether it is even necessary for such information to be removed from the control of the school jurisdiction** (e.g. should the data be stored on a USB stick, on a laptop, or in the cloud to begin with?).

2. The jurisdiction must **restrict unsanctioned onsite wireless internet and network access points** within the jurisdiction. Such connections if not secured provide ideal access points for hackers to access network data.

PRIVACY BREACH

1. School Principals and Division managers shall work with the FOIP Coordinator when issues arise under the scope of the FOIP Act including a determination for the need to notify those individuals whose personal information was subject to inadvertent disclosure.

    (a) Employees shall report incidents (loss, theft, or unauthorized access of personal information and other security incidents) involving personal information immediately to their supervisor and the Horizon FOIP coordinator.

In the event of a privacy breach (lost or stolen device and or confidential data), employees should immediately contact the Jurisdiction FOIP coordinator (John Rakai – Associate Superintendent) who will respond to the breach by:

- **Evaluating the risks** associated with the breach, including a **determination on whether notification is necessary** to avoid or mitigate harm to a student or employee;

- **Investigate the cause** of the breach;

- **Inform** Horizon's FOIP coordinator (John Rakai);

- Develop or **improve** adequate long term **safeguards** against further breaches. Such alterations and/or additions to the safeguards should be communicated to all Horizon employees.

ATTACHMENT #4

Horizon School Division # 67
COMMUNICATION: SOCIAL MEDIA, WEB BASED, DIVISION OWNED DEVICES ADMINISTRATIVE GUIDELINES

Objective:
Horizon School Division supports learning environments that contain cloud based communication and collaboration technology that supports pedagogy and engages and empowers all students and breaks down barriers to inclusive learning. The division also recognizes the statutory and ethical responsibility for staff and students to adhere to citizenship in a digital age guidelines and procedures.

Definitions:
Web Based – can be thought of as what people are doing while online rather than a technology or cloud based application. Web Based Communication is often synonymous with **Social Media** which are the online tools and technology that people use to share opinions, insights, experiences, and perspectives with each other. In both cases the intent is to:

- makes the web faster (e.g. AJAX – asynchronous updates),
- enhances accessibility (e.g. RSS – "really simple syndication"),
- simplifies publishing (e.g. blogging), and
- connect and collaborate with friends and colleagues (e.g. social networks).

In many cases, information is stored remotely in cloud based applications and cloud based data storage facilities and shared within and beyond schools' physical boundaries.

- **Cloud-based applications** are applications hosted outside of Horizon's internal network facilities. Examples include productivity applications to produce and/or store documents, videos, or other forms of expression, but also include "social" applications that facilitate the sharing of information, photos, videos, opinions, and discussion.

- **Cloud-based data storage facilities** are data storage services that provide data storage on servers that are outside the Horizon's internal network facilities.

    - Cloud based applications and cloud based data storage facilities typically require an account before being able to access them or before information can be stored.

    - Some cloud based applications allow you to choose your preferred level of security (e.g. public access, private, or by invitation only).

Background Information:
Advantages

- Meaningful collaboration between students
- Meaningful collaboration between divisional staff
- Opportunity to extend learning to project-based approaches
- Tools are easy to use and work with (user friendly)
- Higher level of student engagement
- Availability of multitude of creation-based tools

- Integration of multi-sensory, multiple intelligence learning and extends scope of differentiated instruction (providing variety of learning choices)
- No cost or minimal cost for software
- Web-based storage- frees space on internal servers and hard drives
- Many web based tools allow you to save back-ups of your work
- Allows anytime access for anytime learning
- Prepares students for the digital world in which they are in
- Potential for further, purposeful and effective integration and uses of technology in core subject areas
- Opportunity to address and continually reinforce Citizenship in a digital age

Disadvantages

- Email accounts are needed for registering for most web based tools
- Potential loss of information if site is no longer in service or no longer is appropriate
- Potential lack of supervision if students are using tools at home
- If standards are not in place and Citizenship in a digital age is not continually reinforced, students may give personal information that is not appropriate
- Cannot be monitored 24/7
- Once posted online, control and management is lost
- Some tools have age restrictions (typically 13) so teachers need to read the user agreements.

Teacher preparation prior to using web based Communication with students:

- Deep understanding of Citizenship in a digital age- how to model and teach good Citizenship in a digital age to students on a continual basis rather than a "one time shot"
- Clear learning outcomes are matched with the activity, and the particular tool is used by the teacher before allowing student access
- Clear classroom guidelines and expectations while using tools with pre-determined consequences beforehand
- Horizon sponsored email accounts will simplify the process and would allow for easier access to usernames and passwords, as web based tools require an email account.
- Read the terms of use agreement on each site- paying special attention to age requirements and other restrictions.
- Parental consent as per FOIP will be needed for students' photos and work posted on websites.
- Make sure that you know how to use the tool efficiently before you open it up to your students.
- Teacher-directed use of cloud-based applications or cloud-based storage by students must be preceded by:
    - Instruction on the terms of use under which the application is being provided by the source,
    - instruction in citizenship in a digital age,

    - communication with parent(s) and/or guardians regarding the instructional value of student use of cloud-based applications and/or storage,
        - Note this consent does not need to be on an application-by-application basis
- Use of cloud-based applications must adhere to age-restrictions,
- Use of cloud-based applications or cloud-based storage by staff must respect the principles of "Citizenship in a digital age". In addition, staff are expected to respect the following while on-line:
    - the same principles of conduct that would be expected while off-line,
    - for all staff, ensure that if you identify yourself as a Horizon employee, that you also clearly articulate that you are not speaking on behalf of Horizon School Division, but are instead expressing a personal view or opinion (unless you are explicitly empowered to speak on behalf of Horizon),
    - for all staff, understand that your actions both on and off line away from work can affect your employment relationship with Horizon.

Student Preparation and expectations for the use of web based learning tools:

- Teachers should read the user agreements for each web based site (and model this process with students)
- Internet safety and classroom guidelines must be established and agreed upon with consequences given beforehand for non-compliance.
- Define web based tools (See http://en.wikipedia.org/wiki/Web_2.0)
- When creating usernames for their web based tool (during initial sign up of tool) students should use on online screen name such as blueman67 or billybob that is unique to themselves, and does not give away their identity to external parties.
- Web based tools will be signed up for using student email accounts. **At no time are students to use their first name or last name when signing up for third party email or web based accounts other than when providing their Horizon email address.** Account user names should not be identifiable outside of the learning environment.
- Students should create a complex password (not a dictionary word) containing a capital letter, lower case letter, a symbol, and/or number somewhere in their password. ***Keep a record of their passwords in a secure area in case they forget, or you want to access their accounts**.
- Keep a record of your student's user-names for the year. If you are using multiple web based tools it might be useful to have students use one pseudonym for the entire year.
- Students use the tools allocated to them through classroom instruction which meet the curricular fit.
- When/if they are instructed to enter an address they enter the address of the school or division office 6302 56 St. Taber AB T1G 1Z9. only, and should not enter their own.
- It is strongly encouraged that all web based tools, have parental consent, and without reference to the "student" or their names.
- Student will not refer to another person in online text inside/outside of the class using that another student's last name. Nor will they give out personal information about themselves or others.

- When signing up for web tools, students will use the following birthdate: 01-01-1967 instead of having use their own.
- Some web based tools require you to confirm email address. In those situations the students would be able to go into their own email accounts and confirm their own web tool enrolment.

Notes:

- Students should be encouraged to create an on-line persona or alias. This is not to be confused with taking on someone else's identity or trying to be someone else. Rather it is teaching them that it is smart to create an online name for themselves to keep their identity safe, similar to a pen name. Students must be taught the difference between an alias for themselves and pretending to be someone else to encourage ethical and responsible Citizenship in a digital age.
- There may be circumstances when student pictures or student identities may enhance the learning project, or give a higher sense of ownership. In these situations it is important to get individual consent for each public activity, just as we do now for media such as newspapers.
- While cloud based accounts are not considered owned by Horizon School Division, access by supervisors will only occur with reasonable cause.
-

Maintaining professional boundaries in all forms of communication, technology-related or not, is vital to maintaining the public trust and appropriate professional relationships with students, parents, and other stakeholders. Employees must be aware of the numerous challenges and the ramifications associated with the use of electronic communication and social media.

This guideline supports the *Teaching Quality Standards for the Teaching Profession* and encompasses all staff within Horizon. Staff express their commitment to students' well-being and learning through positive professional influence, professional judgment and empathy in practice. Honesty, reliability and moral action are embodied in the ethical standard of integrity.

Electronic communication and social media can be effective when used cautiously and professionally. They serve a range of purposes, from helping students and parents/guardians access assignments and resources related to classroom studies to connecting with classrooms in other communities and countries.

Employees also use the Internet and social networking sites as instructional tools and for professional development, seeking information on lesson plans, new developments and methodologies. However, the most popular social media applications were not created specifically for educational purposes and their use can expose employees to risk when it comes to maintaining professionalism. It is up to employees to know and respect proper professional boundaries with students, even when students initiate electronic interaction.

PRIVATE VS. PROFESSIONAL

There is a distinction between the professional and private life of a teacher and the work and private life of all staff. Horizon staff are individuals with private lives, however, off-duty conduct matters. Sound judgment and due care should be exercised. Teaching is a public profession. Canada's Supreme Court ruled that teachers' off-duty conduct, even when not directly related to students, is relevant to their suitability to teach. Employees should maintain a sense of professionalism at all times – in their personal and professional lives.

PROFESSIONAL VULNERABILITY

Employees can be vulnerable to unintended misuses of electronic communication. Social media encourage casual dialogue. Even the most innocent actions can be easily misconstrued or manipulated. The immediacy and simplicity of a text message, for example, may lead to longer, informal conversations. Rules may relax and informal salutations may replace time-respected forms of professional address.

Electronic messages are not anonymous. They can be tracked, misdirected, manipulated and live forever on the Internet. Social media sites create and archive copies of every piece of content posted, even when deleted from online profiles. Once information is digitized, the author relinquishes all control.

The use of the Internet and social media, despite best intentions, may cause employees to forget their professional responsibilities and the unique position of trust and authority given to them by society. Employees should never share information with students in any environment that they would not willingly and appropriately share in a school or school-related setting or in the community. Online identities and actions are visible to the public and can result in serious repercussions or embarrassment.

MINIMIZING THE RISKS: ADVICE TO EMPLOYEES

INTERACT APPROPRIATELY

- Model the behaviour you expect to see online from your students.
- Alert students to appropriate online behaviour and the proper use of comments and images.
- Maintain your professional persona by communicating with students electronically at appropriate times of the day and through established education platforms (for example, a web page dedicated to a school program, project or class rather than a personal profile).
- Maintain a formal, courteous and professional tone in all communications to ensure that professional boundaries are maintained.
- Avoid exchanging private texts, phone numbers, personal e-mail addresses or photos of a personal nature with students.
- When utilizing social media, reflect upon whether one should decline student-initiated "friend" requests and issuing "friend" requests to students for non-school related social media.
- Notify parents/guardians before using social networks for classroom activities. Let them know about the platforms you use in your class to connect with students and consider giving them access to group pages.

UNDERSTAND PRIVACY CONCERNS

- Operate in all circumstances online as a professional – as you would in the community.
- Manage the privacy and security settings of your social media accounts. Privacy settings can shift and change without notice. Check the settings frequently.
- Assume that information you post can be accessed or altered.
- Ensure that the privacy settings for content and photos are set appropriately and monitor who is able to post to any of your social media locations. Remember, no privacy mechanism is guaranteed.
- Monitor regularly all content you or others post to your social media accounts and remove anything that is inappropriate.
- Consider asking others not to tag you on any photographs without your permission.
- Ask others to remove any undesirable content related to you.

ACT PROFESSIONALLY

- Consider whether any posting may reflect poorly on you, your school or the jurisdiction, or the teaching profession.
- Be transparent and authentic. Use your true professional identity at all times. Even if you create a false identity, courts can compel disclosure of your true identity.
- Avoid online criticism about students, colleagues, your employer or others within the school community.
- Avoid impulsive, inappropriate or heated comments.
- Ensure that your comments do not incite others to make discriminatory or other professionally unacceptable comments.
- Respect the privacy and confidentiality of student information.
- Be aware of your employer's applicable policies and programs regarding the use of social media/e-communications and the appropriate use of electronic equipment. Even if your employer has no applicable policy, it is your responsibility to exercise good judgment.

IMPORTANT QUESTIONS TO ASK YOURSELF

- When interacting electronically am I using electronic communication and social media to enhance their learning or to satisfy a personal need?
- What are my reasons for sharing this information – are they professional or are they personal?
- Is this picture or comment something I would be comfortable with my students, their parents/guardians, my supervisor, my family or the media seeing?
- Would my peers or supervisors consider what I have posted as reasonable and professional?
- Would I communicate this way in my community?
- Are the photos, videos or audio recordings I am posting susceptible to misrepresentation or manipulation?
- Am I keeping current in my awareness and knowledge of social media technology developments to protect myself from misuse?

Employees should be able to answer this: How does my online presence – that which I control and that which is posted by others – reflect my professionalism, and how does it reflect on the teaching profession?

Maintaining professional boundaries in all forms of communication, technology-related or not, is vital to maintaining, respect, the public trust and appropriate professional relationships.

GUIDELINES ON CELLULAR PHONE/DEVICE ACQUISITION AND USE

Horizon School Division –Division Office Funded Cellular Phones

Purpose and Scope

The purpose of this guideline is to:

- provide guidance to Horizon School Division employees regarding the proper procurement, use and possession of cellular devices for voice and data communication;
- ensure that the use of cellular technology is correctly authorized and appropriate; and
- ensure that the Horizon School Division is correctly reimbursed for excessive personal use of cellular devices.

Cellular devices are provided to improve service and to enhance business efficiencies. They are an effective resource and enable communication in areas or situations where conventional landline phones are not available or are impractical. They are not a personal benefit and shall not be a primary mode of communication unless they are the most efficient and cost effective means to conduct business.

Cellular phones and services may be provided to certain employees for three principal reasons:

1. The employee performs the majority of his/her job activities "in the field," where business either cannot be conducted on a landline telephone or where it would be inefficient to use a landline telephone. Examples include staff whose daily assignments take them to various sites both throughout the jurisdiction and beyond.
2. The employee's responsibilities require that he or she be immediately accessible in case of emergency.
3. The employee's responsibilities periodically require travel or emergency contact availability.

Procurement

All cellular devices and services, funded from Jurisdiction resources, must be justified on the basis of work assignments and must be approved by the employee's supervisor. No employee may approve his/her own cellular service plan.

All new and renewing service contracts must be done through the transportation administrative assistant

The equipment chosen shall be the most cost efficient option that will provide the required level of service.

The lowest-cost service plan available to accommodate the particular business need of the employee shall be utilized. From time to time, the jurisdiction (with assistance from the service provider) may review individual usage and modify cellular plans to review and ensure cost efficiency and employee compliance with division guidelines.

Procurement of replacement phones may only be done with approval from the employee's supervisor and must be processed through the transportation administrative assistant.

Use of Cellular Devices

The Horizon School Division provides cellular devices to employees for the purpose of conducting jurisdiction business. Employees should realize that, although personal calls made within the local calling region and under the usage limits provided by the employee's plan do not result in additional charges, they do count toward the overall air time usage limits established under the service agreement and should therefore be kept to a minimum.

Long distance personal calls should be avoided if at all possible or redirected to the users' home phone account using a personal calling card.

Employees are asked to reimburse the division for long distance or overage charges deemed unnecessary by the employee's supervisor.

Safe Keeping

Each employee shall be responsible for the safe keeping, care, and custody of the cellular device assigned to him or her.

Cellular phones, telephone numbers and accessories (including chargers, batteries, hands-free devices, cases, and manuals) shall remain the property of Horizon School Division # 67 and shall be relinquished by the employee upon termination of their employment, reassignment to another position, or at the request of the employee's supervisor.

Supervisors shall notify the transportation administrative assistant who shall ensure the service is cancelled or transferred to an approved employee.

Management of Use

Supervisors who become aware of a violation of the letter or spirit of this guideline shall take such remedial action as may be appropriate to control any such violation.

ATTACHMENT #5

Horizon School Division # 67

CONNECTIVITY: WIRELESS AND BRING YOUR OWN DEVICE ADMINISTRATIVE GUIDELINES

Wireless

Objective:

Horizon School Division provides access to a Local Area Network, and internet via a wireless environment for teaching and increasing and enriching student's learning.

Background:

Horizon School Division currently has 3 wireless controllers.

- W.R. Myers' which controls all jurisdiction access points within Taber, Grassy Lake and Barnwell
- Vauxhall High School's which controls all jurisdiction access points within Vauxhall Hays, Enchant, and Lomond
- Erle Rivers which controls all jurisdiction access points within Milk River and Warner

Guidelines:

1. Schools with wireless access points have the ability to access two types of network access: divAP, and openHorizon. Schools wishing to have extensive wireless access points or customized settings are required to acquire their own controller (approx. value $3000).

2. There are two types of networks accessible via the wireless access points

    a. divAP

        (1) School technological devices

        - Provides wireless internet access to all division owned computers (possessing a wireless adapter), laptops, tablets (e.g. Ipad), and smartphones.

        - Provides wireless access to U:// drive (personal drive on the server) to all division owned computers (with wireless adapters) Note: tablets (e.g. Ipad) and smartphones will not have U://drive access.

        (2) Staff owned technological devices

        - provides wireless internet access to staff owned devices (possessing a wireless adapter), including laptops, tablets (e.g. Ipad), and smartphones

        - provides wireless access to U:// drive (personal drive on the server) to all division owned computers (with wireless adapters) and laptops. Note: it does not provide wireless access to U:// drive for staff tablets (ie Ipad), and smartphones (ie Iphones).

- **Staff wishing to access internet using this network are required to provide their device's MAC address to the Technology Department**

- Note: personal computers with windows home version, as opposed to the corporate pro version, are unable to wirelessly access the U:// drive as they are limited by their operating software, and are thus unable to be registered on the jurisdiction's domain and active directory.

b. openHorizon

(1) Provides wireless internet access to any jurisdiction and/or personal device (possessing a wireless adapter), such as a laptop, tablet (ie Ipad), or Smartphone (ie blackberry, Iphone) as long as the user has the encrypted jurisdiction password (empoweringlearners).

- openHorizon does not provide access to the U://drive

- MAC addresses are not required to be submitted to the Technology Department

3. In all cases the internet traffic travels through the jurisdiction's internet and email filtering hardware and/or software: meaning that websites and email are filtered as they would be using wired computers – some sites are overridable by teachers (ie blogs) and some are permanently blocked (ie pornography).

4. The technology department has bandwidth monitoring and packet shaping infrastructure that will allow real-time viewing and archived usage by schools, individual computers, and users. This will facilitate the technology department's efforts in striving to be effective and efficient in terms of bandwidth usage and provide more flexibility in terms of access to specific sites.

5. It should be noted that wired computers have dedicated bandwidth while wireless devices connecting to an access point share its bandwidth allocation. Wireless access is thus, typically slower than wired as multiple devices are sharing one network line.

6. The jurisdiction's bandwidth shaping infrastructure will allow the jurisdiction to provie access to specific sites during specific times.

7. **Special Situations (shared network infrastructure with Vauxhall Academy of Baseball (VAB))**

a. Horizon shares its network infrastructure with the VAB. It is the intent that VAB will have both wired and wireless access points within the dorm (using VHS' controller). This means that both wired and wireless access points access the internet via the jurisdiction's local area network and are bound by the same restrictions as all other users and computers within the jurisdiction.

Bring Your Own Device

Objective:
Horizon School Division believes students' ability to bring their own device may enrich student's learning.

Guidelines:

1. Within Horizon School Jurisdiction we:

    a. have jurisdiction and school policies in place regarding students' use of technology (whether school or personally owned) and access to the internet

    b. provide a filtered internet service

    c. provide supervision, direction, and support in online activities using wired and wireless technologies for learning

    d. support students in developing digital literacy skills and citizenship in a digital age

2. All parents and students must sign that they understand and will abide by the **Terms and Conditions** within the Acceptable and Responsible Use Agreement before students are granted access to the division's network (wired and wireless).

3. Teachers are encouraged to regularly review the **Terms and Conditions** within the Acceptable and Responsible Use Agreement with their child and parents.

4. Parents/guardians should be aware that the nature of the internet is such that full protection from inappropriate content can never be guaranteed.

5. Horizon School Division provides access to a Local Area Network, internet and technology as teaching and learning tools that must be used responsibly.

6. Wireless access is provided free of charge. If a student does access the internet through their personal account via their smartphone or other personal technology with a data plan, all charges become the responsibility of the account holder. This does not exempt students from appropriate behaviours as outlined in these administrative guidelines.

7. Citizenship in a digital age, which includes safe and responsible behavior, is essential in the lives of students and is best taught and reinforced in partnership with parents.

8. Today’s students spend increasing amounts of time online, learning and collaborating. To be safe online and to gain the greatest benefit from technology and the opportunities provided through an online environment, students need to learn to do the right thing whether they are supervised or not. Learning and citizenship within a digital age does not stop at the school door.

9. Inappropriate online activities, such as cyber-bullying, will not be tolerated. Horizon School Division #67 expects that its students, staff, volunteers, and students respect and protect themselves, others, and intellectual property All activities that go against the concept of citizenship in a digital age will be dealt with swiftly and thoroughly.

ATTACHMENT #6

Horizon School Division # 67

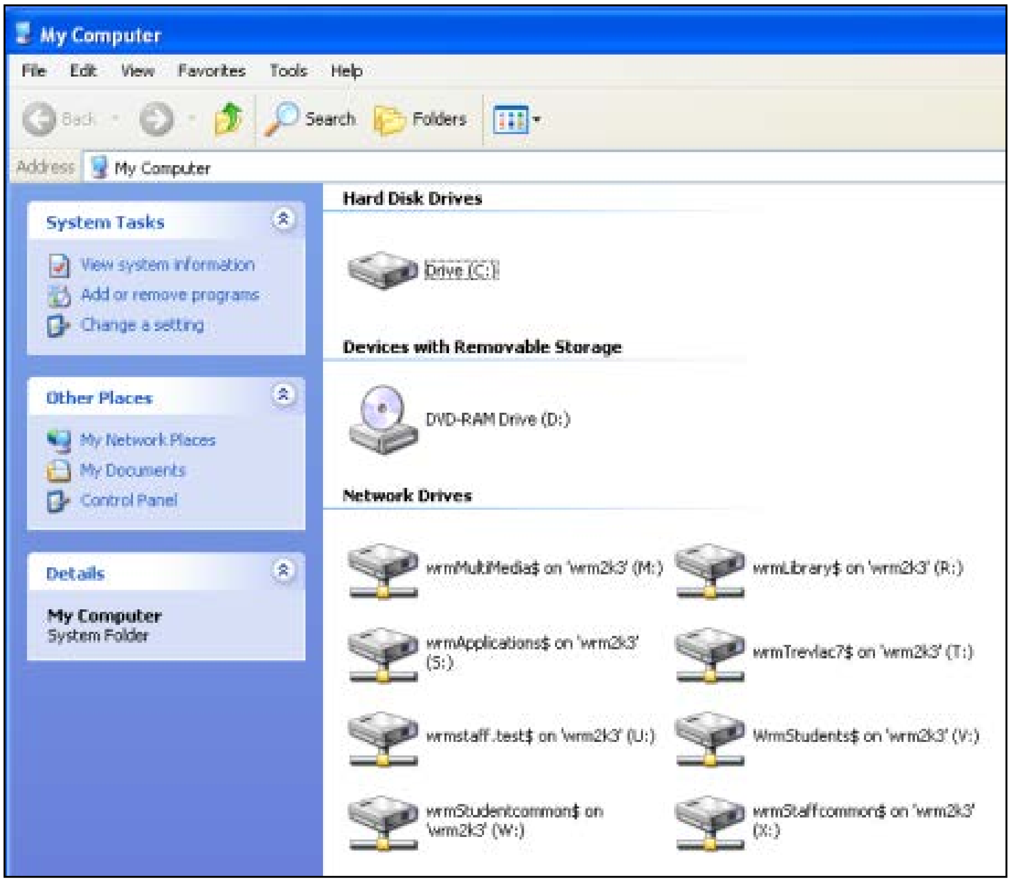
STANDARD OPERATING PROCEDURES

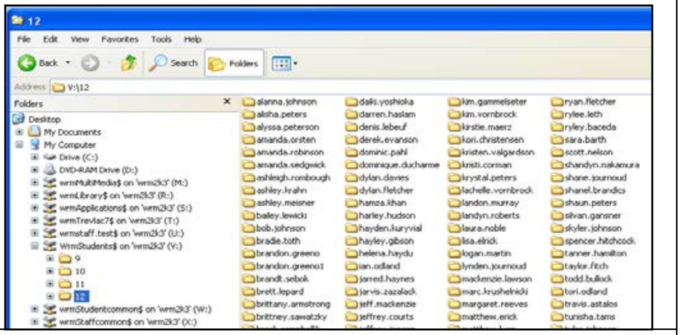
TECHNOLOGY STANDARD OPERATING PROCEDURES

1. General Computer, Network, and Internet Access
   - Horizon provides technology to support and enhance learning and teaching in a manner that allows for the attainment of the outcomes from the Program of Study and the development of citizenship in a digital age.
   - NOTE: usernames have an 18 character limitation, thus should staff or student names exceed this they will be truncated. There is also a limitation regarding spaces (they are not allowed and thus will be removed).

2. Network Access
   - Staff
     - The Technology department automatically creates network accounts for new staff when they are hired. Normally the username is their firstname.lastname and a temporary password "three uppercase letters representing school)

       ACE for ACE Place
       ATL for Arden T. Litt
       BAR for Barnwell School
       CEN for Central School
       CHA for Chamberlain School
       COL for all colony schools
       DAF for D.A. Ferguson Middle School
       DRH for Dr. Hamman School
       ENC for Enchant School
       ERH for Erle Rivers High School
       HAY for Hays School
       LOM for Lomond School
       LTW for L.T. Westlake School
       MAP for Horizon Mennonite Alternative School
       MAP for Taber Mennonite School
       MRE for Milk River Elementary
       TCS for Taber Christian School
       VES for Vauxhall Elementary School
       VHS for Vauxhall High School
       WAR for Warner School
       WRM for W.R. Myers High School
     - This password should be changed as soon as staff log on for the first time. Should a staff have difficulty logging on to the network, they can phone the Technology Department 223-3547 or via email help@horizon.ab.ca
     - NOTE: when staff log on they will have access to the school's server and a personal folder *U Drive* (U:) in which to store personal files (accessible from any computer you logon to). There is also a *Staff Common* (X:) where staff can temporarily store files that they would like to share with other staff within their school (this is not a long-term storage location) and a *Horizon Common* (J:) where staff can temporarily store files that they would like to share with other staff across the jurisdiction.
     - Files should NOT be saved on local hard drives as these are not backed up (unlike the server folder). As well computers may be reimaged without notice, thus information stored on local hard drives is prone to being lost and/or deleted.



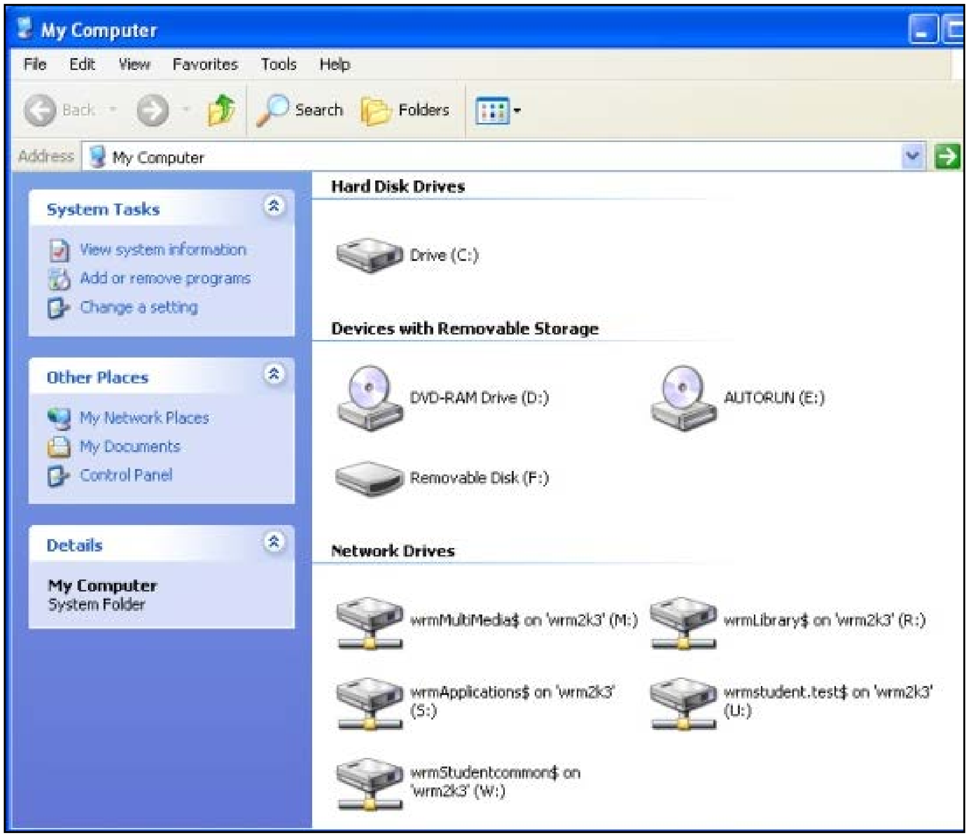
Drives	Name	Description
(J:)	Horizon common	One folder shared by all staff across the jurisdiction so that they can share files between schools. Files placed in this folder are accessible and modifiable by all staff from any Horizon school. This is a temporary storage location that is deleted each summer.
(U:)	Teacher's personal folder	A personal network drive. This folder is backed up daily and follows staff's profile (accessible from any Horizon computer).
(V:)	Student folders	Contains all students personal folders sorted by grade. Student folders are deleted each summer so students should be reminded to save files they wish to keep before year end. 
(W:)	Student common	One folder shared by all students so that they can share files between each other and staff. Files placed in this folder are accessible and modifiable by anyone. This is a temporary storage location that is deleted each summer.
(X:)	Staff common	One folder shared by all staff within a school so that they can share files between each other. Files placed in this folder are accessible and modifiable by all staff within their school. This is a temporary storage location that is deleted each summer.

Remote Access for staff

- While the jurisdiction has no licensed remote access ability, there are free apps that can be installed on iPads and personal computers such as "Team Viewer"

Student

- Student network access is automated. As soon as secretaries enter students in Powerschool a network account is created (should be operational by Sept 2013). Students can access the network by logging in using their username which is normally their firstname.lastname and a temporary password "three uppercase letters representing school – ie CHA) that students should change as soon as they log on for the first time. Should a student experience difficulty logging on to the network, their teacher can phone the Technology Department 223-3547 or via email help@horizon.ab.ca
- NOTE: when students log on they will have access to the school's server and a personal folder in which to store personal files. There is also a *studentcommon* where students can temporarily store files that they would like to share with other students and/or staff (this is not a long-term storage location). Files should NOT be saved on local hard drives as these are not backed up (unlike the server) and are occasionally reimaged, thus information is prone to being lost and/or deleted. It is also important to note that student files on servers are deleted annually during the summer so students should be reminded that any files they wish to save should be backed up on a personal USB stick or other storage device.

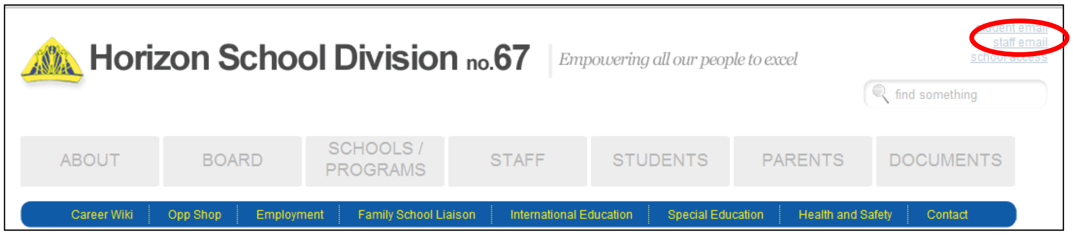


Drives	Name	Description
(M:)	Multimedia	
(R:)	Library	
(S:)	Applications	
(U:)	Student's personal folder	A personal network drive. This folder is backed up daily and follows student's profile (accessible from any Horizon computer).
(W:)	Student common	One folder shared by all students so that they can share files between each other and staff. Files placed in this folder are accessible and modifiable by anyone. This is a temporary storage location that is deleted each summer.

3. Email

Staff

- Horizon utilizes a customized Google mail system for staff email. Should horizon's website go down staff can still access their emails by going directly to https://mail.google.com/a/horizon.ab.ca
- The Technology department automatically creates email accounts for new staff when they are hired. Normally this is their firstname.lastname@horizon.ab.ca and a temporary password (first three letters of their school, twice followed by 12 – e.g. ACEACE12). Staff should change this password as soon as they log on for the first time. Should a staff have difficulty logging on to their email account, they can phone the Technology Department 223-3547 or via email help@horizon.ab.ca

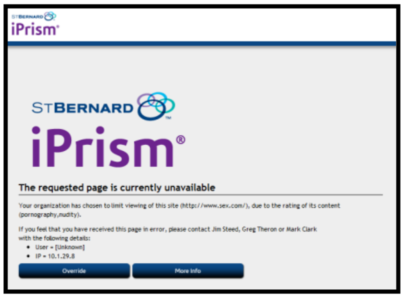


Student

- Student email access is automated. As soon as secretaries enter students in Powerschool an email account is created (should be operational by Sept 2013). Students can access this account via the link in the top right menu of the horizon homepage (www.horizon.ab.ca)
- Normally this is their firstname.lastname@hsd67.ca and a temporary password "three uppercase letters representing school, repeated once – ie CHACHA) that students should change as soon as they log on for the first time. Should a student have difficulty logging on to their email account, staff can phone the Technology Department 223-3547 or via email help@horizon.ab.ca

4. Staff override of Internet filtering

- Horizon has a filtering system (iPrism – StBernard) that blocks inappropriate sites. Staff have the ability to override this blockage for a short duration by entering their username and password (same username and password as for logging onto the network) should they wish to access the blocked site. Staff are reminded that students should not gain access to your password as it will allow students to access teacher folders and files.

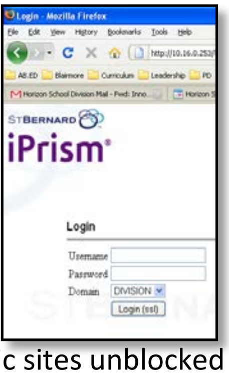


The requested page is currently unavailable

Your organization has chosen to limit viewing of this site (http://www.sex.com/), due to the rating of its content (pornography,nudity).

If you feel that you have received this page in error, please contact Jim Steed, Greg Theron or Mark Clark with the following details:

- User = [Unknown]
- IP = 10.1.29.8

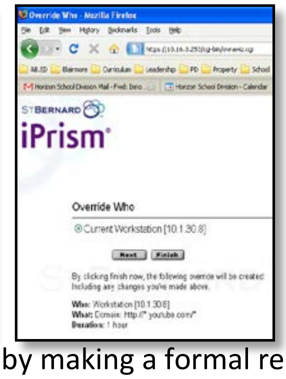

Login - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://10.16.0.253/
AB.ED Blairmore Curriculum Leadership PD
Horizon School Division Mail - Fwd: Inno...
Horizon S
STBERNARD iPrism

Login

Username

Password

Domain DIVISION


Override Who - Mozilla Firefox
File Edit View History Bookmarks Tools Help
AB.ED Blairmore Curriculum Leadership PD Property School
Horizon School Division Mail - Fwd: Inno...
Horizon School Division - Calendar
STBERNARD iPrism

Override Who

◉ Current Workstation [10.1.30.8]

By clicking finish now, the following override will be created including any changes you've made above.

Who: Workstation [10.1.30.8]
What: Domain: http://*.youtube.com/*
Duration: 1 hour

- Staff can request to have specific sites unblocked by making a formal request to the Associate Superintendent of Curriculum and Instruction via the school principal.

5. Requesting technological assistance

- Simply send an email to help@horizon.ab.ca and elaborate the details of your issue.

6. Jurisdiction Wide Technology Resources

- Horizon subscribes to a number of online resources that assist teachers in their practice. Some of these require authentication. A list follows:
  - http://www.discoveryeducation.ca/Canada/ This site provides access to a large quantity of videos that can be streamed live or downloaded for later viewing. Staff should contact the Associate Superintendent of Curriculum and Instruction should they want access to these.

Discovery Education supports teachers in accelerating student achievement, bringing the wonder of Discovery into classrooms to ignite students' natural curiosity.

  - http://www.learn360.com the premier website for K-12 multi-media educational resources. Teachers can use generic accounts or request personal accounts to access over 73,000 media resources from trusted educational publishers and producers. Access is acquired via school username: xxxteacher and school password: xxxteacher where xxx is either ACE, ATL, BAR, CEN, CHA, DAF, DRH, ENC,ERH, HAY, MAP, LTW, LOM, MRE, VES, VHS, WRM, WAR.

LEARN360
ENGAGE • ENRICH • EXCEL
LOGIN
NEW USERS
Username
Password
Forgot username or password?
LOGIN
Remember Me
HOME
ABOUT US
FUNDING
CONTENT
SERVICES
NEWS
National Diabetes Awareness Month
Educating Students About Diabetes
Click Here to Learn More...

Welcome to Learn360, the premier website for K-12 multi-media educational resources.

Sign up for a FREE 30-day trial today to gain access to over 73,000 media resources from trusted educational publishers and producers, which will ENGAGE your students, ENRICH their learning experiences and drive them to EXCEL both inside and outside of the classroom.

Redefine your Classroom Today!

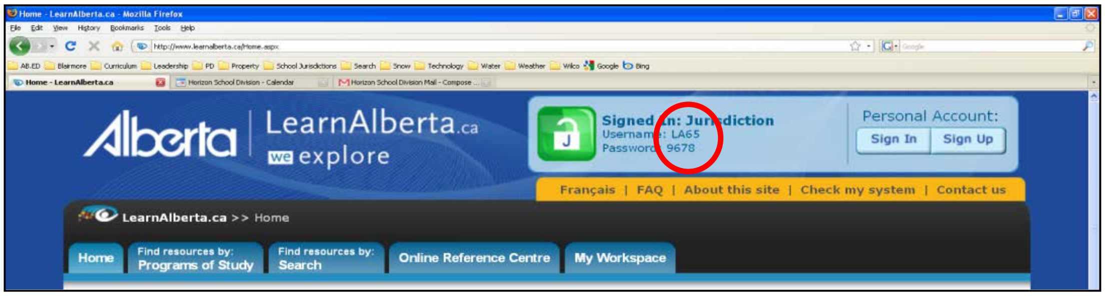
- http://www.accesslearning.com Canada's leading provider of educational media. Teachers can use generic accounts or request personal accounts to access over 3,500 full length and 20,000 clip level educational video programs. Access is acquired via school username: xxxteacher and school password: xxxteacher where xxx is either ACE, ATL, BAR, CEN, CHA, DAF, DRH, ENC,ERH, HAY, MAP, LTW, LOM, MRE, VES, VHS, WRM, WAR.

accesslearning
Parents & Students Click Here
Schools & Teachers Click Here
Visit us on Facebook & Twitter!
About Us | Contact | Distribution Access
Login
User Name :
Password :
Login
Forgot Username Or Password?
Promo Code :
GO
Interested in a free trial?
Access Learning News
accesslearning
EDUCATION WITH VISION
1
2
3
4

Welcome to Access Learning

Over 3,500 videos and 20,000 video clips addressing K-12 topics and applications to the real world.

- http://www.learnalberta.ca/ Teachers can create personal accounts using their teaching certificate number. Access can also be acquired for jurisdiction students There is an automated system in place for jurisdiction computers and they automatically have student specific access. Logging in from non-jurisdiction computers will require the specific username and password. This account changes annually and individuals are encouraged to log on to jurisdiction computers to acquire the latest username and password (see red circle below). Staff experiencing difficulty should contact the technology department 223-3547 or help@horizon.ab.ca .



Signed In: Jurisdiction
Username: LA65
Password: 9678

- http://www.aac.ab.ca/ Horizon is a member of the Alberta Assessment Consortium which provides teachers with a plethora of resources focusing around assessment. Access is acquired via username: Horizon and password: Learning

7. Cisco VoIP Phones

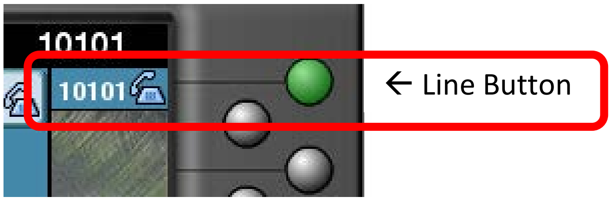
- Horizon Schools utilize a Voice over Internet Protocol (VoIP) Phone system commonly referred to as an IP phone. These phones, while connected to traditional phone lines utilize the internet instead of traditional phone lines in many situations and thus eliminate, or reduce the need for long distance charges
- There are a variety of IP phones models within the jurisdiction and schools have the option of customizing their phone system's features thus some components of this section may not apply or might vary somewhat.
- Schools can communicate free of charge from with one another via IP phones by dialing a 5 digit extension number.
    - The first two numbers refer to the school
    - The last three numbers refer to the extension
        - 105 is the principal
        - 104 is the secretary
        - 167 is typically the VC suite phone (some exceptions apply)
        - First 2 digits of extensions are as follows:

Division Office	10	D.A. Ferguson	23	Lomond	43
Taber Maintenance	11	Dr. Hamman	25	Milk River Elementary	32
A.C.E. Place	20	Enchant	40	Taber Christian	29
Arden T Litt		E.R.H.S.	31	V.E.S.	44
Barnwell	21	Hays	41	V.H.S.	45
Central	27	Horizon M.A.P.	42	W.R. Myers	22
Chamberlain	24	L.T. Westlake	26	Warner	33

- To Place a call
    - With in the school division, pick up the handset or press the speaker phone button 🔈 then dial the extension number.
    - Outside the school division, pick up the handset or press the speaker phone button 🔈 then dial 9 (or 6) then the number. Eg. 9-1-403-310-0000
        - Dialing **9** selects one of the school telephone lines and dials out from the school.
        - Dialing **6** selects one of the jurisdiction telephone lines located in Taber and dials out from Taber (This may reduce the need to incur long distance charges.) NOTE: dialing 6 is limited to local calling.
        - Note that calling 911 requires you to dial 9-911 (as you need to select a phone line first)
    - From division speed dial list pick up the handset or press the speaker phone button 🔈 then dial * and the speed dial choice. Eg. *01 will dial Barnwell.
    - One can also just dial the number and then pick up the handset or press the speaker phone button 🔈

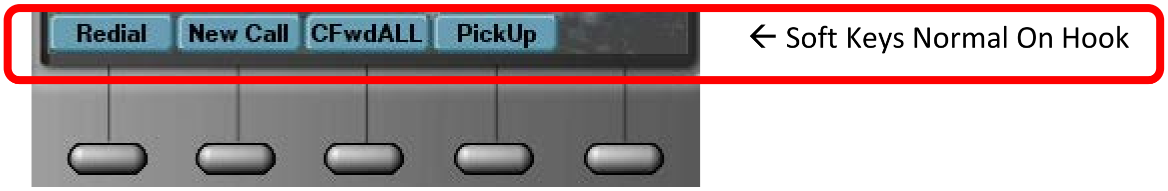
⚠ To answer the phone.

- Pickup the handset or press the speaker phone button 🔈 or press the line button this automatically turns on speaker phone unless you have the receiver off hook.

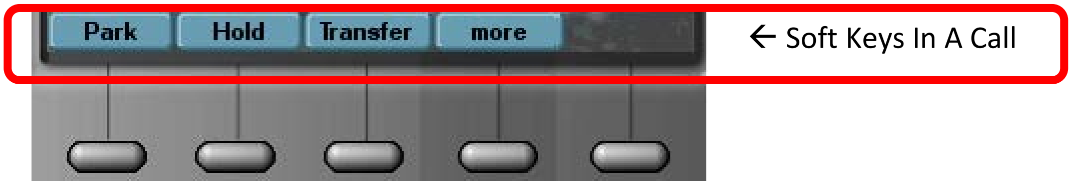


← Line Button

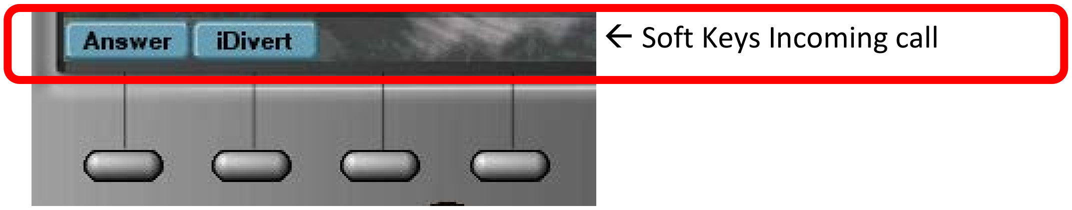
⚠ To use Soft keys Hold, Park, Transfer and More.
(Cisco Phones like new cell phones have Soft keys that change depending on the use of the phone.)



← Soft Keys Normal On Hook



← Soft Keys In A Call



← Soft Keys Incoming call

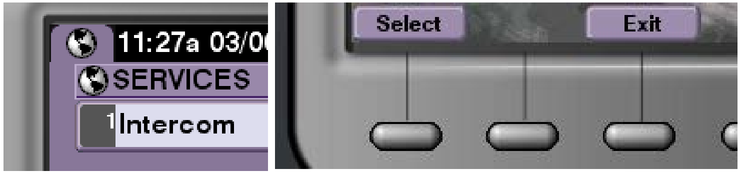
- Park is the method used to enable someone to place a caller on hold and have someone else answer the call on another phone. When you park a call you will be given a park number this is the number needed to retrieve the call from hold. ***Eg. You don't know where the person the callers asking for is in the building so you need to page for them to pick up the phone you press the park softkey and are presented with ie 10770 as the park number. Then you page the person to pick up line 10770. If unanswered the call will ring back in 60sec.***
- Transfer is used to direct a call to a specific extension. To transfer a call press the transfer Soft Key and then dial the extension they are trying to reach. At this point you have two options ***A. asks the person at the extension you have just dialed if they would like the call. If they say yes then press the transfer key again.*** Or ***B. Press the transfer key again and the call will be transferred immediately if there is no answer there, voicemail will answer.***
- Park or Transfer are the preferred call handling methods, but hold is also useful. When you are in a call you can press the hold soft key. The caller is now on hold

and the line light is blinking green. You can now call someone else, make it a conference call or retrieve the call by pressing the green blinking line button.

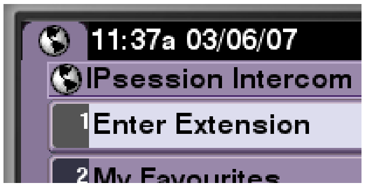
- Don’t want to be bugged with calls? No problem just press the CFwdALL (Call Forward) soft key and then press the Voicemail Button.
    - Now all calls go straight to voicemail.
    - Press CFwdALL again and your calls are unforwarded.

Other available services

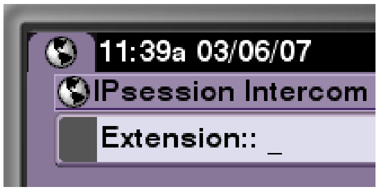
- Paging
    - To perform a page dial #99 say your message and hangup.
    - Eg. I have parked a call for Mark on line 10774 and I don’t know where he is in the building, so I need to page him. I dial #99 (this number may vary between schools) and say mark line 10774 and hang up.
- Intercom.
    - Press the Services Key
    - Select the Intercom service from the services menu by pressing 1 or the select softkey.



    - From the IPsession Intercom services menu, choose Enter extension by pressing 1



    - Now type the extension Number of the person you wish to intercom to and press the submit button.



    - When you are done hang up call.
    -
- Directories Button
    - Gives you a list of Missed calls, Received Calls, Placed Calls, and a Corporate Directory.
    - To use the Corporate Directory press the Directories Button and select option 4
    - You have three options here: First name, Last Name, Number.

    - To do a search by first name type the first the first few letters of the persons name
    - Eg: gre and then press the search soft key.
    - A listing of extensions will show up. Select the appropriate one with the rocker key
    - The press the Dial soft Key

- Voicemail (8*extension#password#)
    - To retrieve your voicemail there are two options
        - Press the Voicemail button on your Phone
        - Dial the main horizon phone number from any phone and press **8** when you hear the menu
            - press *****
            - then enter your **extension** followed by **#**
            - then enter your **password** followed by **#**
    - The temporary password is 473671 and can be changed when you do your setup.

- Voicemails are normally deleted. However since IP phones are more like a computer deleting them is like placing them into the trash on a computer. As such, you should regularly empty your trash.

    - Press the Voicemail button on your Phone
    - Enter your password followed by #
    - Press 3
    - Press 2
    - Press 2
    - Press 1
    - Press 2

- Voicemail Menus
    - Press 1 Play new messages

      1 repeat
      2 save
      3 delete
      5 forward
      6 mark new
      7 skip back
      9 message properties
      * Exit
    - Press 2 send a message

    *Exit

- Press 3 Review old messages
    - 1 saved messages
    - 2 deleted messages
    - *Exit
- Press 4 settings
    - A. Greeting’s
        - 1. Rerecord standard greeting
        - 2. Alt Greeting on and off
        - 3. Edit Other Greetings
            - 1. Standard Greeting
            - 2. Closed Greeting
            - 3. Alt Greeting
            - 4. Busy Greeting
            - 5. Internal Greeting
            - 6. Holiday Greeting
            - *. Exit
        - 4. Play All Greetings
        - *. Exit
    - B. Message settings
    - C. Personal settings
    - D. Transfer settings

8. Video Conferencing and Bridgit

- Horizon has VC capabilities in all of the communities around the jurisdiction.
- Using the Video Conferencing Suite.
    - To use the V/C suite, find and use the VC remote. To turn the V/C unit on, point the remote at the front of the V/C camera and press the power button. Once the camera begins to move you can use the projector remote to turn on the projector. When you see an image from the projector, you can press the “Source Search” button on the projector remote until you see the video conferencing screen (you should see the room you are in on the screen).
    - From this point use the VC remote to perform all V/C functions.
    - From the on-screen menu choose the phonebook or if you know the number to dial enter it in the “IP” box at the bottom of the first screen. If someone will be calling to your location you need to do nothing else other than turn on the V/C unit and select the V/C display on the projector you have chosen.

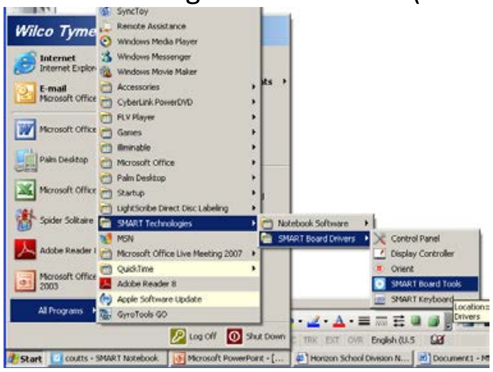
Location	Dialing Number	IP Phone
AB Ed	7997242530@199.213.3.202	
Blairmore	99@192.139.33.50	
Holy Spirit	4997239555@199.213.7.177	
Leth College	4995134435@199.185.123.112	
ACE PD	4993223178@199.213.6.70	10047

Barnwell	4993223146@199.213.6.70	21167
Central	4993223027@199.213.6.70	27167
Coutts	4993223114@199.213.6.70	30167
Chamberlain	4993223194@199.213.6.70	24123
Div Office	4993223242@199.213.6.70	10035
Warner	4993223098@199.213.6.70	33167
Enchant	4993223130@199.213.6.70	40167
Hays	4993223056@199.213.6.70	41167
Lomond	4993223162@199.213.6.70	43167
Vauxhall	4993223034@199.213.6.70	45167
WR Myers	4993223018@199.213.6.70	22009

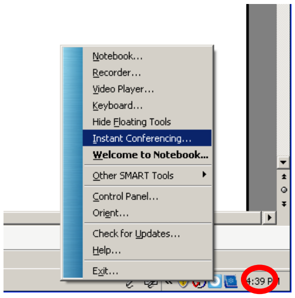
- Note: to enter @ hit the “alpha/num” key and then the “symbol” key twice. You do not need to dial @199.213.6.70 if dialing from one school to another

Creating a Bridgit Session

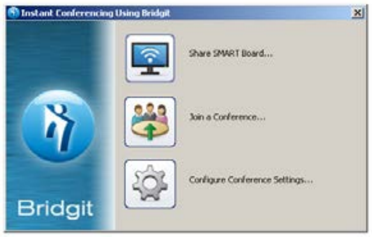
- Open Smartboard Tools using the Start menu (see image below)



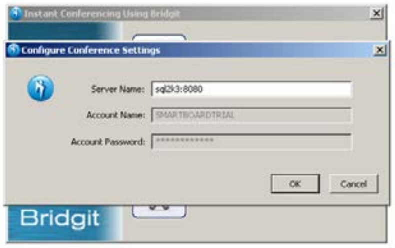
- Click on the *Smartboard icon* in the system tray (bottom left) and click on *“Instant Conferencing”*



- When you click on *“Instant Conferencing”* the following window will appear.


Instant Conferencing Using Bridgit
Share SMART Board...
Join a Conference...
Configure Conference Settings...
Bridgit

- Before you can share your smartboard you may have to *"configure conference settings"* by clicking on this phrase
  - You will need to enter **sql2k3:8080** in the server name box and click *"OK"*

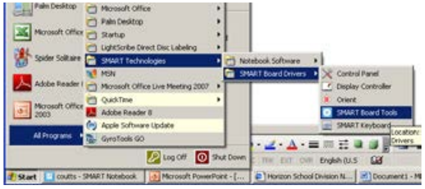

Instant Conferencing Using Bridgit
Configure Conference Settings
OK
Cancel
Bridgit

Server Name: sql2k3:8080
Account Name: SMARTBOARDTRIAL
Account Password: ************

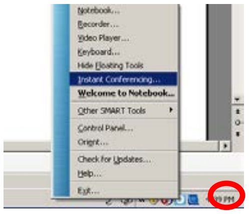
- You can now click on "share smartboard"
  - Enter a conference name (can be anything)
  - Enter a password (**horizon**)
  - Enter your name

Joining a Bridgit Session

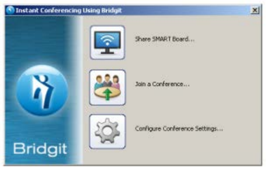
- Open Smartboard Tools using the Start menu (see image below)



- Click on the *Smartboard icon* in the system tray (bottom left) and click on *"Instant Conferencing"*

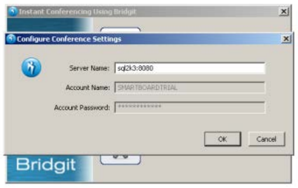


- When you click on *"Instant Conferencing"* the following window will appear.


Instant Conferencing Using Bridgit
Share SMART Board...
Join a Conference...
Configure Conference Settings...
Bridgit

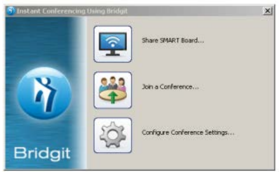
- Before you can join a conference you may have to *"configure conference settings"* by clicking on this phrase

- o You will need to enter **sql2k3:8080** in the server name box and click *"OK"*

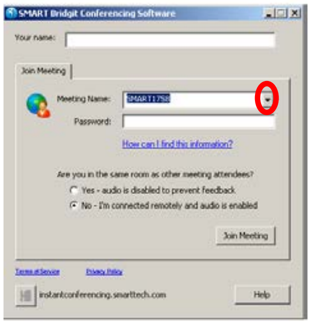

Instant Conferencing Using Bridgit
Configure Conference Settings
OK
Cancel
Bridgit

Server Name: sql2k3:8080
Account Name: SMARTBOARDTRIAL
Account Password: ************

- You can now click on *"join a conference"*

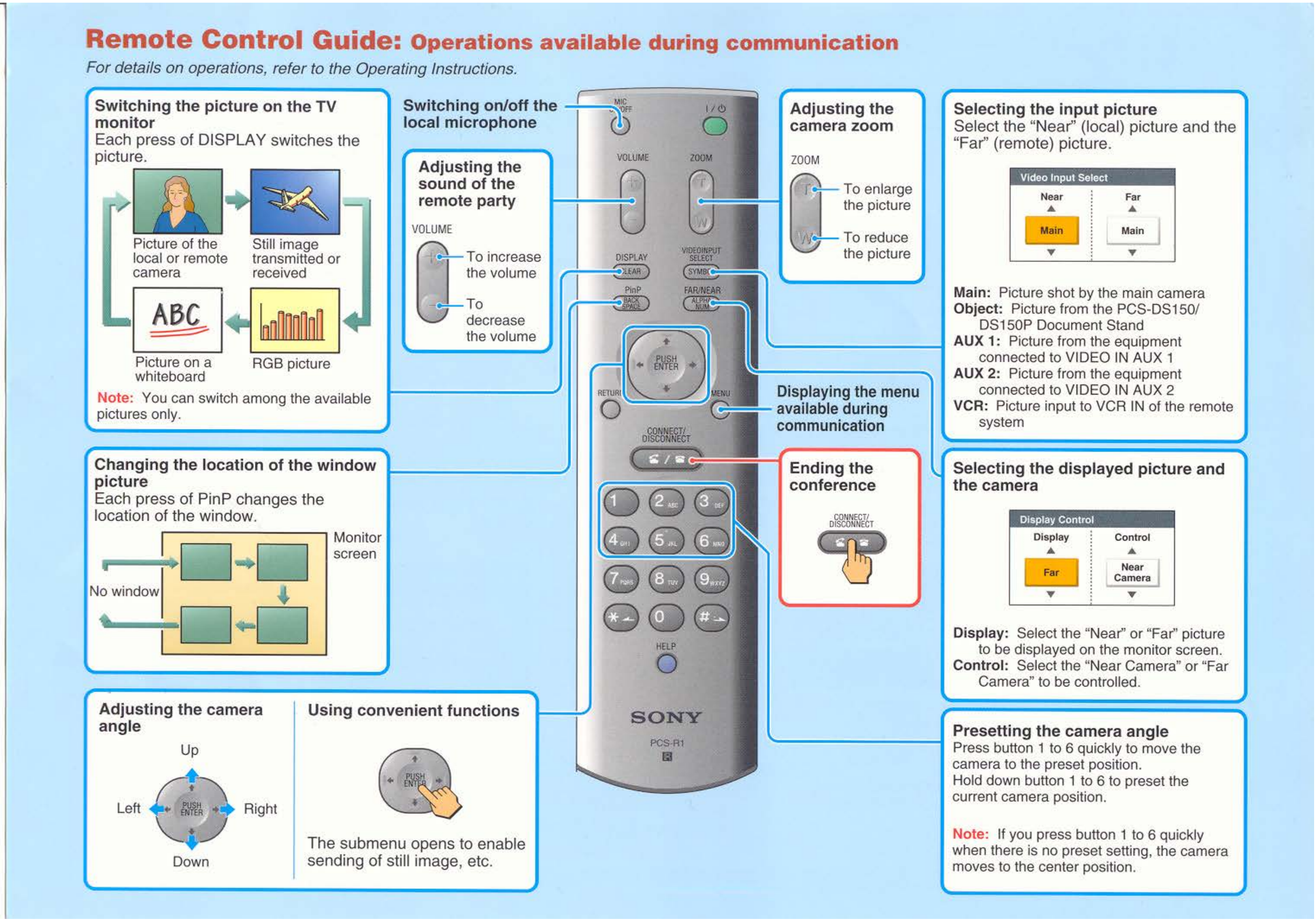

Instant Conferencing Using Bridgit
Share SMART Board...
Join a Conference...
Configure Conference Settings...
Bridgit

- A new window will open up
  - o Enter your name
  - o Go to the down arrow (red circle) and choose the meeting name that you want to join
  - o Enter the password (horizon)
  - o Click on *"Join Meeting"*


SMART Bridgit Conferencing Software
Join Meeting
How can I find this information?
Join Meeting
Terms of Service
Privacy Policy
instantconferencing.smarttech.com
Help

Your name:
Meeting Name: SMART1758
Password:

Are you in the same room as other meeting attendees?
○ Yes - audio is disabled to prevent feedback
● No - I'm connected remotely and audio is enabled



Remote Control Guide: Operations available during communication

For details on operations, refer to the Operating Instructions.

Switching the picture on the TV monitor
Each press of DISPLAY switches the picture.

Picture of the local or remote camera
Still image transmitted or received
Picture on a whiteboard
RGB picture
ABC

Note: You can switch among the available pictures only.

Switching on/off the local microphone

Adjusting the sound of the remote party

To increase the volume

To decrease the volume

Adjusting the camera zoom

To enlarge the picture

To reduce the picture

Selecting the input picture
Select the "Near" (local) picture and the "Far" (remote) picture.

Main: Picture shot by the main camera
Object: Picture from the PCS-DS150/ DS150P Document Stand
AUX 1: Picture from the equipment connected to VIDEO IN AUX 1
AUX 2: Picture from the equipment connected to VIDEO IN AUX 2
VCR: Picture input to VCR IN of the remote system

Displaying the menu available during communication

Ending the conference

Selecting the displayed picture and the camera

Display: Select the "Near" or "Far" picture to be displayed on the monitor screen.
Control: Select the "Near Camera" or "Far Camera" to be controlled.

Changing the location of the window picture
Each press of PinP changes the location of the window.

Adjusting the camera angle

Using convenient functions

The submenu opens to enable sending of still image, etc.

Presetting the camera angle
Press button 1 to 6 quickly to move the camera to the preset position.
Hold down button 1 to 6 to preset the current camera position.

Note: If you press button 1 to 6 quickly when there is no preset setting, the camera moves to the center position.

SONY

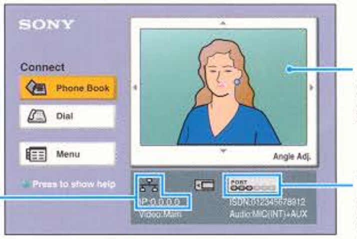
Video Communication System

Quick Connection Guide Using the Phone Book

For details on operations, refer to the Operating Instructions.

To begin with

Turn on your Video Communication System and TV monitor, and check the following to ensure that connection is possible.



When using the LAN
Is the LAN indicator dark and is the IP address displayed?

Is the picture of your camera (local picture) on the monitor screen?

When using the ISDN
Are one or more ports of the ISDN indicator dark?

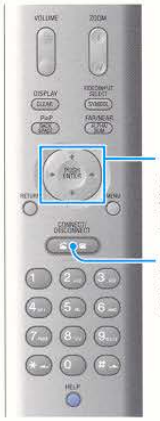
Note: Connection to a remote party is impossible if neither the IP address nor ISDN indicator is displayed.

Main indicators that appear during communication

FAR	Controlling a remote camera
MIC OFF	Local microphone is cut off
	Sending a still image
	Receiving a still image
	Sending or receiving an image of a computer
	Sending or receiving data of a whiteboard

After checking...

Let's connect

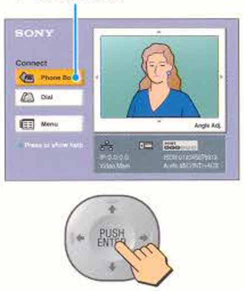


↑/↓/←/→ (arrow) buttons and PUSH ENTER button

CONNECT/DISCONNECT button

1 Select "Phone Book" and press PUSH ENTER.

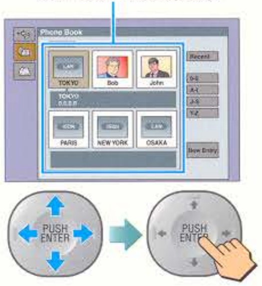
"Phone Book"



Use ↑/↓ to select "Phone Book" if it has not been selected.

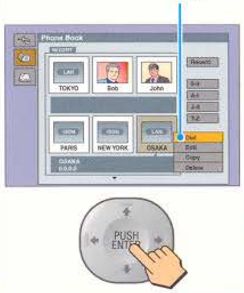
2 Select a remote party, and press PUSH ENTER.

Select a remote party.



3 Dial to the remote party.

"Dial"



Or

Select a remote party.

PUSH ENTER
CONNECT/DISCONNECT

Press.

4 The system dials automatically, and establishes communication.

Dialing(LAN)
OSAKA
0.0.0.0
Cancel
Meeting starts!

If the remote party is not registered in the Phone Book
Call a remote party manually, referring to the Operation Guide.

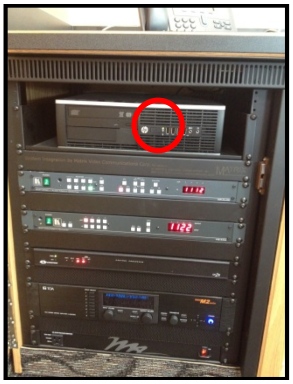
If communication cannot be established after a number of trials
The line registered in the Phone Book may not be used. Consult your system administrator.

3-836-775-11(1)

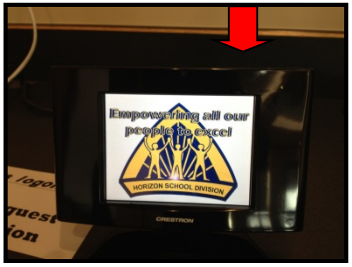
9. Eric Johnson Room Technology

Computer

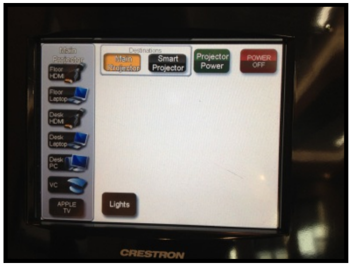
- Can be turned on by opening the cupboard and pushing the on button. PLEASE DO NOT TOUCH ANY OF THE OTHER CONTROLS as they have been calibrated.



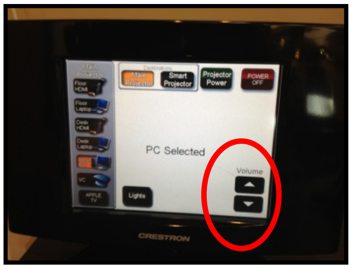
- Log in is the same as any other computer
- USB devices can be connected to the computer using the USB ports on the front of the computer in the cupboard.
- Volume can be adjusted via the computer or the main control unit on the counter (NOT using any of controls inside the cupboard).
    - Push the button on the top of the main control panel (left or right side) to acquire the Horizon logo



    - Push the main screen to acquire the selection screen



    - Once the main projector or SMARTboard projector is selected volume can be adjusted on the bottom right of the screen



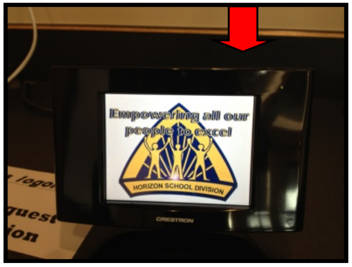
- Please ensure that the Mouse is placed on the charging cradle after the computer is no longer in use

Laptops

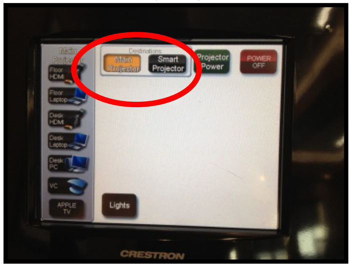
- Laptops can be connected to the system using the cables on the countertop by the main computer or using the floor jack at the front of the room.

Projectors

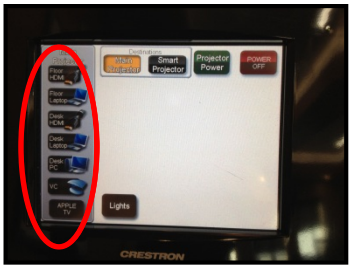
- Once the computer is on (or a laptop is connected to the system) the Main control unit on the counter is used to project the computer image onto the screen
    - The image can be on the Main projector screen, the SMARTboard projector screen or both
    - Push the button on the top of the main control panel (left or right side) to acquire the Horizon logo



    - Push the main screen to acquire the selection screen and chose the main projector or SMARTboard projector

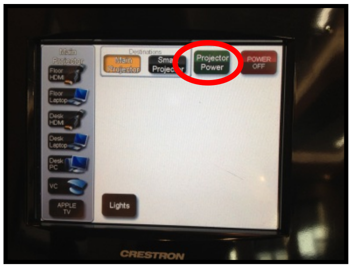


    - Then select the computer using the choses along the left hand side

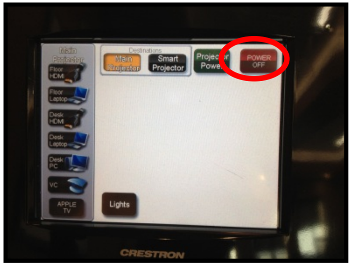


  - The Projector screen will automatically come down, lights will be dimmed and the image will appear.

- The Projectors can be turned off individually by pushing the projector power button

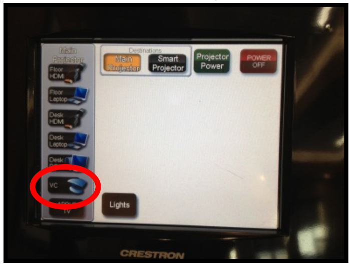


- or the whole system can be turned off by pushing the top right red button

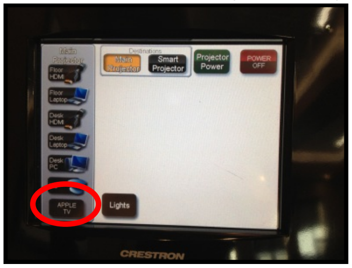


Additional Data Sources

- VC Unit – push this to be able to dial up and utilize the VC Unit

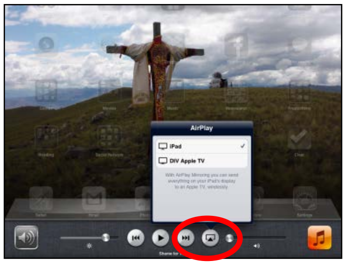


- Apple TV – use this to connect wirelessly to an Ipad image.



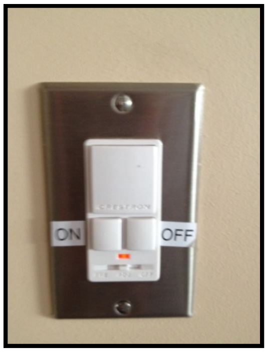
  - Ensure the Ipad is connected to the wireless network

    - Double click the home button and slide the bottom banner to the volume settings. You will notice a button to the right of the play button
    - Turn on mirroring

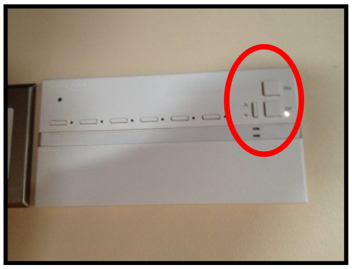


With AirPlay Mirroring you can send everything on your iPad's display to an Apple TV wirelessly.

- Lights
  - Lights can be controlled one of three ways
    - Automated – preprogrammed settings are activated when the main projector, SMARTboard, or VC unit are turned on.
    - Wall controls
      - Main Entrance Wall Controls

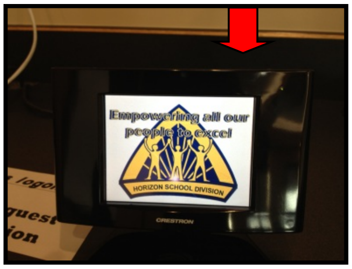


        - Large button turns on back potlights
        - Left turns ON all lights
        - Right turns OFF all lights
      - Computer Station Wall Controls

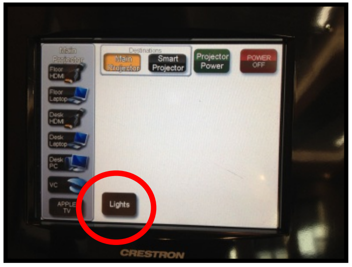


All lights can be turned off or on using the buttons on the right side of the control panel (Please DO NOT use the left *zone* buttons) these are for dimming and the lights are not dimmable. (if these controls are used the lights will flicker).

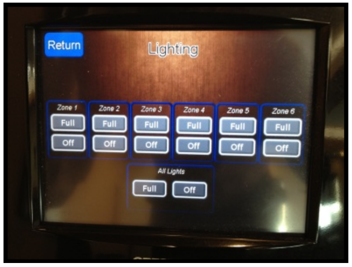
      - Master Control Unit on the counter
        - Push the button on the top of the main control panel (left or right side) to acquire the Horizon logo



- Push the main screen to acquire the selection screen
- Push the *lights* button on the bottom of the screen



- Select the zones you want on or off



- Push *return* to return to the main menu