Nipissing-Parry Sound Catholic District School Board	**USAGE OF THE BOARD'S COMPUTER NETWORK AND INTERNET**	**AG 34.0**

Policy Section	*Original Approval Date*	*Revision Date(s)*	*Review Date(s)*
Administration - General	**June 27, 2000**	**July 29, 2015** **August 13, 2019** **September 2, 2020**	**n/a**

POLICY

The Nipissing-Parry Sound Catholic District School Board ("the Board") endorses the use of existing and emerging technologies to promote educational excellence, 21st century learning competencies, and professional development, work productivity and cooperation through resource sharing, access to information and communication.

Consistent with this vision, the Board provides access to its computer network to staff and students. Services on the network include the following, although all services may not be available to all users:

- electronic mail (E-mail);
- access to the Board's electronic services, such as Staff Portal, Student Information Systems, Human Resources/Payroll and Financial Services;
- access to the Internet;
- secure remote and wireless access to the Board's network via secure socket layer (SSL).

The Board is committed to using reasonable care to prevent injury or damage from danger which is, or ought to be, known to the Board, and to see that the premises provided for the accommodation of school children are as safe as reasonable care can make them.

In providing access to a global network, the Board recognizes its limitations in fully controlling access to inappropriate information and interactions. The Board has taken reasonable precautions to restrict access to controversial materials.

The users of the Board's network are required to adhere to the following terms and conditions to ensure responsible use of the Board's computer network.

REGULATIONS

1. Definition

The Board's network is defined as the set of electronic platforms and devices operated and administered by the Nipissing-Parry Sound Catholic District School Board to facilitate communication and records management

These facilities and devices include, but are not limited to, computers, tablets, handheld devices, routers, switches, telephones and data lines registered under the Board's name. In addition, any computer session involving any set of these devices will be deemed part of the network and subject to this agreement.

2. Acceptable Use

Use of the Board's network and Internet must be consistent with the Board's *Policy E1 – Ends*, its mission and vision, and educational objectives of the Board. The use of technology and the Board's network must support a culture of respect, equity and inclusion, and promote values consistent with Catholic teachings. Furthermore, use of other organizations' networks or computing technology resources must also comply with the rules appropriate to those networks.

3. Ownership Of Data

The Board owns all communication sent, received, and stored via its network infrastructure.

4. Reliability

The Board makes no warranties of any kind, whether expressed or implied, for the services it is providing. The Board will not be responsible for any damages suffered by the user and assumes no responsibility or liability for any phone charges, line costs or usage fees, nor for any damages a user may suffer. This includes, but is not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or the user's errors or omissions.

Use of any information obtained via the Board's network is at user's risk. The Board specifically denies any responsibility for the accuracy or quality of information obtained through its services.

5. Security

a) Network Security

Security on any computer system is a high priority, especially when the system involves many users. If a user identifies a security problem on the network, they must notify the IT Service Desk immediately.

b) User Security

Users must maintain secure passwords as outlined in the Board's Password Guideline.

Users must not reveal any personal information relating to themselves or others. (Also refer to *Appendix 3 - Cloud Computing (Green and Red Environments)*)

Users must not reveal their login/password to anyone. If they do, they are responsible for any misuse by another user. If they believe that another user has attempted to, or has used their account without authorization, they must notify the IT Service Desk immediately.

Users must screen lock their computers when left unattended.

c) Illegal Activities

Illegal activities must be reported. Report any illegal activities to the appropriate authorities immediately.

6. Prohibited Activities

a) Any illegal activities are strictly prohibited. This includes, but is not limited to the following:

i. transmission of any material in violation of any law or regulation such as copyright materials, cyber-bullying, threatening or obscene material, or material suggesting pornography, racism, sexism, or discrimination of any kind;

ii. use of the network to devise or execute any scheme to defraud;

iii. vandalism, such as any malicious attempt to damage or destroy equipment, software, data of another user, the Board's network, or any other network connected to the Internet;

iv. intentionally uploading, downloading, or creating computer viruses;

v. attempting to access unauthorized resources, entities, or data;

b) Activities inconsistent with educational objectives:

vi. Personal (also refer to *Policy AG 34.2 – Use of Electronic Social Media*)
vii. commercial use;
viii. political lobbying;
ix. cyber-bullying, harassment or nuisance messages.

c) Activities that waste, degrade, or disrupt network resources or performance.

7. Digital Citizenship

Users are expected to abide by the generally accepted rules of digital citizenship. These include, but are not limited to, the following:

a) be polite;

b) do not write or send annoying or abusive messages to others;

c) do not invade the privacy of others;

d) use appropriate language; do not swear or use vulgarities;

e) send only information that one would convey in other media (privacy of E-mail messages cannot be guaranteed: maintenance of the E-mail system may require access to users' files)

f) recognizing that computer resources are limited and valuable, ensure file transfers meet educational objectives of the Board;

g) stay on topic and keep messages short and to the point.

h) adhere to *Employee Mobile Technology: Support and Usage Guidelines* (refer to Staff intranet's *Information Technology* page).

i) maintain good cyber security practice:
   i. Know the risks are there and you are not immune.
   ii. Practice good password management. Adhere to *Guidelines for Network Password Management* (refer to Staff intranet's *Privacy Information Management* page).
   iii.
   iv. Never leave your device unattended.
   v. Always be careful when clicking on attachments or links in email.
   vi. Only access sensitive data, such as banking, on devices and networks you trust.
   vii. Back up your data regularly, and make sure your anti-virus software is always up to date.
   viii. Avoid sharing sensitive information.
   ix. Be conscientious of what you plug into your computer.
   x. Do not share confidential data with anyone requesting information on the phone or via email.
   xi. Monitor your accounts for any suspicious activity.

8. Enforcement of Terms and Conditions

The use of the Board's network is a privilege, not a right. Penalties for violation of these terms and conditions may range from temporary or permanent withdrawal of privileges, to prosecution under the law.

The Network Administrator may close an account at any time, as required.

9. Application for Account

a) Students

Annually, students of the Board must apply for a network account by submitting a completed application form and contract (*Appendix 2*) to their school Principal or designate.

Your signature on the attached contract is legally binding and indicates the parties who signed have read the terms and conditions carefully and understand their significance. Students under eighteen (18) years of age will require a parent/guardian signature on their agreement.

b) Staff

Initially, staff of the Board must apply for a network account by submitting a completed application form and contract (provided in this policy) to the Network Administrator, Information Technology department.

Your signature on the attached contract is legally binding and indicates the parties who signed have read the terms and conditions carefully and understand their significance.

In all subsequent years, staff of the Board must complete the online network agreement declaration by October 31st of each school year to retain their network account.

10. Representing NPSC Schools on Social Media

NPSC employees and volunteers representing all or a part of NPSC and it's schools on the Internet or in social media are legally bound by this policy and *policy AG 34.2 Use of Electronic Social Media* (also refer to *Appendix 3 - Cloud Computing (Green and Red Environments)*).

Related Guidelines

- *School Web Publishing Guidelines for the NPSC Network* (section 11 of this policy).
- *Guidelines for Network Password Management* (refer to Staff intranet's *Privacy Information Management* page).

Related Policies

- AG 34.1 Use of Hand-held Devices While Driving
- AG 34.2 Use of Electronic Social Media
- AG 28.0 Records Management
- PB 10.0 – Collection, Protection of and Access to Personal Information of Private Individuals and-or Board Employees
- AG 20.0 – Use of Copyright and Fair Dealing

11. School Internet Publishing Guidelines on the NPSC Network

a) Basic Principles

School Internet publishers on the Board's network are required to adhere to the following guidelines to ensure responsible use of the Board's Internet server and related information. Access to the Internet is funded by the Board to enrich the learning and working environment of students and staff. Accordingly, the Board provides opportunities to publish school information on the Board Internet site.

The Principal of the school will be accountable for the implementation of these guidelines.

i. Digital Citizenship for Internet Publishing

School staff are expected to abide by the general accepted rule of digital citizenship. In addition to the Board's computer network and Internet policy, the following also apply when publishing content to the Internet.

- All postings must comply with the Board's policies including but not limited to, those dealing with code of behaviour, sexual, racial or ethno-cultural harassment.

- All those publishing to the Internet are required to use discretion in their language and behaviour and to show respect for other users and will be held accountable.

- No information that may breach privacy, disadvantage, embarrass, defame or ridicule another user or group of users may be published.

- The publication of any school content on the Internet such as, but not limited to, website, blog, wiki, Twitter account, Facebook page must be in support of education or research and be consistent with the educational objectives of the Board.

- Any link established from Board related pages or documents to an outside organization should be carefully selected in terms of its educational values. Its placement on any school website or social media account should contribute to the educational development of students and/or benefit of the school community and subject to the approval of the school principal.

- Sites must be kept current. Sites found to be obsolete or redundant will be addressed by the Communications Officer.

- When Social Media accounts are created to represent a school such as, but not limited to, website, blog, wiki, Twitter account, Facebook page, an alternate administrative account must be created for central management by the Communications Officer.

ii. Security

Security on any computer system is a high priority, especially when the system involves many users. It is understood that the Internet is not secure and no information should be posted of a sensitive or personal nature. Internet distribution is worldwide and the cultural diversity and security of students and their families must be respected (also refer to *Appendix 3 - Cloud Computing (Green and Red Environments)*).

iii. **Vandalism**

Vandalism is defined as any attempt to damage or destroy data of another user or any agencies/networks that are connected to the Internet. This includes, but is not limited to, the intentional posting of files which contain or create computer viruses.

iv. **Copyright**

The school principal is responsible for ensuring that all work posted on the school's website is original or that written permission has been obtained for the use of copyright material and its ownership fully acknowledged.

All communications and information posted to the Internet should be assumed to be intellectual property with all the assigned rights involved.

v. **Consequences**

Inappropriate posting of school websites on the Internet could result in the following consequences and actions:

- Temporary loss of posting privileges
- Permanent loss of posting privileges
- Legal action as appropriate.

vi. **Parent Information**

It is necessary to provide parents/guardians with accurate and appropriate information regarding the educational value and content that will be published within the school's websites.

vii. **Permissions/Release Forms**

For students under sixteen (16) years of age, the school must obtain from the parent or guardian a release form for a student's inclusion in a group, action or individual photo to be published in the school website page. It is recommended that this permission be obtained as part of the registration process. Students in a photo shall be identified only by the first name and last name initial e.g. John D.

b) Posting of School Websites

All school websites hosted on the Board's Network or paid for by the Board are considered to be the property of the Board. Staff from the Information Technology Department will be responsible for managing the Board's website, creating additions and deletions to the site and creating links and ensuring the school website publishing guidelines are followed.

A posting on another Internet Service Provider's website is subject to Board policy *AG 26.0 – News Release to the Media or to the Public*. Accordingly, such postings will require the approval of the Director. The Board's or the school's Universal Resource Locator (URL) should be provided if Board information is required on external servers.

POLICY REVIEW CYCLE

The Board will review this policy on an annual basis.

APPLICATION AND AGREEMENT – STAFF

Directions: After reading the Regulations governing Usage of the Board's Computer Network and Internet, please complete the appropriate sections of the following contract. Please return the contract to the NETWORK ADMINISTRATOR, INFORMATION TECHNOLOGY DEPARTMENT. Questions may be addressed to the Information Technology Department Service Desk at ext. 31251.

I have read pages one through eight of the Regulations governing "Usage of the Board's Computer Network and Internet". I understand and will abide by these regulations. I further understand that violation of the regulations is unethical and may constitute a criminal offence. Should I fail to comply with all the regulations, my access privileges may be revoked and/or appropriate legal action taken.

LAST NAME: _____ FIRST NAME: _____
(Print) (Print)

CIRCLE ONE: TEACHER • ADMINISTRATOR • SUPPORT STAFF

SCHOOL/DEPARTMENT:_____

SIGNATURE: _____

DATE: _____/_____/_____
DD MM YYYY

When your account is established, the Information Technology Department will notify you of your username and user password.

IMMEDIATE SUPERVISOR/HR MANAGER:_____
(Print)

SIGNATURE: _____

DATE:_____/_____/_____
DD MM YYYY

Guidelines for Student Responsible Use of Technology

It is the policy of the Nipissing-Parry Sound Catholic District School Board to endorse the use of existing and emerging technologies to promote educational excellence and that the Internet and the Board's Information Technology are used to support learning in a manner that is consistent with the Board mission and vision statement, Catholic values and strategic directions.

1. Purpose of the Network (LAN/WAN)

- Use of the information technologies owned or operated by the Board must be used for the purpose of enhancing education and instruction and to conduct Board business.
- Use of the Board's Wide Area Network and its connection to the Internet for advertisement or monetary profit must have Board approval.
- The Board will from time to time and without prior notice to the student, access and/or monitor the Board's Electronic Information Systems.

2. Digital Citizenship

- The Board provides access to the Internet for educational activities defined in the teacher instructional plans.
- Users will not post, publish, or display any defamatory, abusive, threatening, sexist, racially offensive, profane, obscene, discrimination based on sexual orientation, illegal and other material found to be offensive.
- The sending or storage of offensive messages from any source is prohibited.
- Users shall not copy information or software in violation of copyright laws.
- Software and resources downloaded will be used only under the terms and conditions specified by the owner or creator of those resources.
- Only authorized staff are to download software, applications ("apps") or executable (.exe) programs.
- It is prohibited for a user to post messages and attribute them to another user.
- Users will not plagiarize works that they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.

3. Vandalism

- Transmission of any software having the purpose of damaging computer systems and files (i.e. computer viruses) is prohibited.
- Any malicious attempt to harm or destroy the data of any person, computer or network linked to the Board's Network is prohibited and will result in financial compensation to the Board and/or the pursuance of criminal charges and/or other disciplinary action consistent with the School Code of Conduct, Board policy and/or legal authorities.
- Users will not attempt to gain unauthorized access to the Board's system or to any other computer system through the Board's system, or go beyond their authorized access. This includes attempting to log in through another person's account or accessing another person's files. These actions are illegal, even if only for the purposes of browsing.

4. Security and Personal Safety

- Users may not share their passwords or accounts with others and must make all efforts to safeguard this information from unauthorized users.
- Users are advised to refrain from giving out personal information, such as their family name, email address, home address, school name, city, country or other information that could help someone locate or contact them in person.
- Users will not post identifying photos, videos, or recordings. Any capture of photo, video or audio recording through the use of any device or sharing/posting of such will only be done with the expressed authorized permission of those involved.
- The Board reserves the right to block access to sites and to conduct regular checks of the system as deemed appropriate.
- An individual search will be conducted if there is reasonable cause to suspect that a user has violated the law, the school code of conduct, and/or the Student Responsible Use of Technology Agreement.
- Personal files are discoverable under public records law.
- Users must screen lock their computers when left unattended.

5. Inappropriate Material

- Unauthorized interactive gaming will not be accessed through the Board Network.
- Upon access to or receipt of material that is educationally inappropriate and contrary to the Board's Mission Statement, the user shall immediately turn off the display and report the incident to the classroom teacher, staff, and/or immediate supervisor.

6. Violations

The principal of the school will deal with violations of the Student Responsible Use of Technology Agreement. Students found in violation of the agreement may face disciplinary action, which may include:

- Suspension from the Board network.
- Revoking access to electronic devices and the Internet on the Board network.
- Suspension from school.
- Paying the cost of any damages/losses resulting from the student's inappropriate use of the resources.
- Referral to the police.

Information Collection Authorization:
The information contained on this form has been collected under the authority of the Education Act R.S.O. 1980, as amended and the Municipal Freedom of Information and Protection of Privacy Act, 1989. Information from this form will be used to enforce appropriate use of the Internet and information technology in accordance with ***Usage of The Board's Computer Network and Internet*** *(AG 34.0) and guidelines attached. The contact person for queries regarding this information is the Supervisor of Information Technology Department or the Superintendent of Education.*

Primary/Junior/Intermediate (JK to Grade 8)

It is the policy of the Nipissing-Parry Sound Catholic District School Board to endorse the use of existing and emerging technologies to promote educational excellence and that the Internet and the Board's Information Technology are used to support learning in a manner that is consistent with the Board mission and vision statement, Catholic values and strategic directions.

STUDENT CONSENT

I agree to:
- Use all technology (i.e.: laptop, Chromebook, netbook, iPad, iPod) carefully and not damage, change or tamper with the hardware, software, the network or any settings.
- Keep my password secret.
- Use the technology for educational purposes and only to help me learn.
- Give credit to the author of work I find on the Internet and obey copyright laws.
- Not provide my personal information (name, address, phone number, photograph) to anyone on the Internet.
- Never meet in person with someone I have met online without my parent's approval and participation.
- Always tell my teacher(s) or other school employees about anything on any device that is inappropriate or makes me feel uncomfortable.
- Never use any form of electronic communications to harass, frighten, or bully anyone.
- Never take and send a picture or video of another person or a group over an electronic network without prior informed permission of all the individuals involved.
- Always consider the environment when deciding what to print by only printing items that are necessary.
- Ensure my behavior adheres to the safe, inclusive and accepting School's Code of Conduct.

For devices I own, I further agree to:
- Protect my device from loss, damage or theft.
- Keep the device up to date, including antivirus, while using NPSC network.
- Not run host servers on my device, including web servers, ftp servers, mail servers, file sharing and peer to peer, while using NPSC network.
- Follow the direction of staff with respect to the use of my personal device.

LAST NAME: _____ **FIRST NAME:** _____
(Print) (Print)

SIGNATURE: _____ **DATE:** _____

PARENT/GUARDIAN CONSENT:
- I have read and understand the Nipissing-Parry Sound Catholic District School Board's Student Responsible Use of Technology Agreement /Guidelines.
- I recognize that this Agreement is designed for my child's grade level and that the full Board policy: ***Usage of The Board's Computer Network and Internet*** (AG 34.0) can be found at www.npsc.ca.
- I will stress the ethical and responsible use of technology and caution my child about unsafe interaction with others on the Internet.
- I grant permission for my child to access networked information technology, including the Internet and email for educational purposes.
- I am aware that my child will be given instruction on the proper use of the Internet at school and further recognize that I am responsible to supervise my child's use of the computer and Internet outside of the school premises.
- I will ensure that media and software on my child's personal electronic device (if applicable) has been purchased and is legal.
- I understand that the School/Board will not service my child's personal electronic device, nor will it be liable in the event that the device is lost, stolen, damaged, or otherwise rendered inoperable.
- I understand that the Board will from time to time and without prior notice to the student access and/or monitor the Board's Electronic Information Systems.

PARENT NAME: _____
(Print)

SIGNATURE: _____ **DATE:** _____

Information Collection Authorization:
The information contained on this form has been collected under the authority of the Education Act R.S.O. 1980, as amended and the Municipal Freedom of Information and Protection of Privacy Act, 1989. Information from this form will be used to enforce appropriate use of the Internet and information technology in accordance with ***Usage of The Board's Computer Network and Internet*** *(AG 34.0) and guidelines attached. The contact person for queries regarding this information is the Supervisor of Information Technology Department or the Superintendent of Education.*

Intermediate/Senior (Grades 9 to 12)

It is the policy of the Nipissing-Parry Sound Catholic District School Board to endorse the use of existing and emerging technologies to promote educational excellence and that the Internet and the Board's Information Technology are used to support learning in a manner that is consistent with the Board mission and vision statement, Catholic values and strategic directions.

STUDENT CONSENT

- I have read and understand the Nipissing – Parry Sound Catholic District School Board's Student Responsible Use of Technology Agreement /Guidelines.
- I agree to abide by the terms and conditions described within this Agreement and the requirements outlined in the attached guidelines and in the following Board policy: ***Usage of The Board's Computer Network and Internet*** (AG 34.0) which can be found at www.npsc.ca.
- I recognize that failure to comply with this Agreement may result in the loss of computer and/or network access privileges, financial compensation to the Board and other disciplinary actions consistent with the School's Code of Conduct, Board policies and/or legal authorities.
- I will ensure my behavior adheres to the save, inclusive and accepting School's Code of Conduct.

For devices I own, I further agree to:

- Protect my device from loss, damage or theft.
- Keep the device up to date and legal, including antivirus, while using NPSC network. (i.e. commercial software has been purchased).
- Ensure that software and firmware is up to date as recommended by the manufacturer, while using NPSC network.
- Not run host servers on my device, including web servers, ftp servers, mail servers, file sharing and peer to peer, while using NPSC network.
- Never use any form of electronic communications to harass, frighten or bully anyone.
- Follow the direction of school staff with respect to the use of a personal electronic device.

LAST NAME: _____ (Print) **FIRST NAME:** _____ (Print)

SIGNATURE: _____ **DATE:** _____

PARENT/GUARDIAN CONSENT:

- I have read and understand the Nipissing-Parry Sound Catholic District School Board's Student Responsible Use of Technology Agreement /Guidelines.
- I recognize that this Agreement is designed for my child's grade level and that the full Board policy: ***Usage of The Board's Computer Network and Internet*** (AG 34.0) can be found at www.npsc.ca.
- I will stress the ethical and responsible use of technology and caution my child about unsafe interaction with others on the Internet.
- I grant permission for my child to access networked information technology, including the Internet and email for educational purposes.
- I am aware that my child will be given instruction in the proper use of the Internet at school and further recognize that I am responsible to supervise my child's use of the computer and Internet outside of the school premises.
- I will ensure that media and software on my child's personal electronic device (if applicable) has been purchased and is legal.
- I understand that the School/Board will not service my child's personal electronic device, nor will it be liable in the event that the device is lost, stolen, damaged, or otherwise rendered inoperable.
- I understand that the Board will from time to time and without prior notice to the student access and/or monitor the Board's Electronic Information Systems.

PARENT NAME: _____ (Print)

SIGNATURE: _____ **DATE:** _____

CLOUD COMPUTING (GREEN AND RED ENVIRONMENTS)

Cloud computing provides users with on-demand access to the Board's online services which may be located on-site or in contracted cloud computing environments, such as, hosted computing resources for the housing of Board computer based services not built by the Board (e.g., Google Apps for Education, Desire2Learn, Office 365, Career Cruising, Synrevoice, etc.). Hosted computing resources may be labelled as Green Sites or Red Sites to inform users of the level of security of the data stored in these sites.

Green Sites

Green Sites are those sites that are under contract and managed by the Nipissing-Parry Sound Catholic District School Board and/or the Ministry of Education. Inappropriate activities (such as cyber-bullying) can be mitigated in a Green Site. Student information (including full student names and assessment data) is safe and secured in the appropriate systems. However, using a Green Site does not take away the onus to maintain personal levels of security over access to the user's materials and passwords. Green Sites include Edsby, Google Apps for Education, Desire2Learn, Office 365, Career Cruising, Synrevoice).

Red Sites

Red Sites are those sites that are not monitored or under contract with the Nipissing-Parry Sound Catholic District School Board and/or the Ministry of Education. Because Red Sites are privately owned and operated, the Board cannot guarantee the same level of security as a Green Site. Staff must take further precautions when using Red Sites. If staff are in doubt about the security of a site not listed as a 'green site' above, contact the Information Technology Department for guidance. Inappropriate activities (such as cyber-bullying, hacking and/or data mining) are difficult to mitigate on a Red Site.

Staff should note that care and consideration needs to be taken when inputting information into a Red Site. Parental permission may be required for student use of a Red Site. As well, data stored in a Red Site would need to be depersonalized in some way (e.g. use initials rather than full names of students). Some examples of Red Sites are Dropbox, Prezi, WordPress, Edmodo, iCloud, Evernote or any sites not on the Green Site list above. While a site may say that 13 years of age is the age of consent of use for their product, the legal age of consent in Ontario for an agreement is 18 years of age.

UNDERSTANDING PRIVACY CONSIDERATIONS VIDEO

See this video for a full understanding of Red and Green Sites: https://youtu.be/xq5K1wSfmeE

Parent – Teacher Electronic Collaboration and Communication

The Nipissing-Parry Sound Catholic District School Board uses many platforms to communicate and collaborate with students and parents. Staff will be using these digital platforms to increase parent engagement. The tools listed below are considered "Green" which means they are Board or Ministry of Education contracted with a specific security and privacy agreements in place:

- Edsby,
- Parent Portal and
- BrightSpace (D2L/VLE)
- Outlook (email)
- SchoolMessenger Communicate

Tools not contracted by the Board or the Ministry of Education do not have security and privacy agreements in place. An example of such a "Red" tool is Remind www.remind.com. If non-contracted tools are used, staff must not share staff and student information with a third party or developer.

E-Mail Based Tools:

In accordance with policy *AG 34.2 Use of Electronic Social Media* and the Canadian Anti-SPAM Legislation, staff are prohibited from using board communication platforms for commercial purposes. All communication from staff to members of the public are expected to adhere to professional standards and relate to educational matters.

Parental Access and Custodial rights:

Before initiating an invitation to participate in guardian summaries, the classroom teacher needs to verify the parent/guardian email address by consulting Edsby Parent or Student Contacts sections for the email address.