See the following pages for exhibits related to electronic communication and data management:

Exhibit A: Designated Campus PEIMS Administrator and PEIMS Data Entry Personnel – 1 page

Exhibit B: Six-Week Grading Period PEIMS Verification – 1 page

Exhibit C: Student Guidelines for Acceptable Use of Technology Resources – 8 pages

Exhibit D: Employee Guidelines for Acceptable Use of Technology Resources – 9 pages

Exhibit E: Board Member Guidelines for Acceptable Use of Technology Resources – 8 pages

Exhibit F: Required Signature Page (Elementary) – 2 pages
- Permission for Publishing Student Work

Exhibit G: Required Signature Page (Secondary) – 2 pages
- Permission for Publishing Student Work

EXHIBIT A

Northwest Independent School District

Designated Campus PEIMS Administrator and PEIMS Data Entry Personnel

Campus	School Year

The following professional and paraprofessional campus personnel have been designated as PEIMS Data Entry Personnel.

My signature acknowledges that I understand and have assumed responsibility for the timely inputting of PEIMS data and the accuracy of that information on all required state and local reports for this campus.

Printed Name of Data Entry Personnel	Signature of Data Entry Personnel	Position	Area of Responsibility
			Enrollment Data
			Attendance Data
			Bilingual Data
			ESL Data
			G/T Data
			Special Education Data (Speech Path.)
			Special Education Data (Speech Path.)
			Special Education Data (Diagnostician)
			Special Education Data (Diagnostician)
			Title I Data
			At-Risk Data
			Pregnancy Program Data
			Membership Summary Data
			Discipline Data
			Discipline Data
			Discipline Data
			Discipline Data
			Discipline Data
			Discipline Data
			Other: _____
			Other: _____

My signature indicates that I understand and assume responsibility for the campus PEIMS data.

Campus PEIMS Administrator's (Print)	Campus PEIMS Administrator's Signature	Date

This form indicates the personnel held accountable for coordinating, inputting, and verifying PEIMS data.

Principal's Signature	Date

Please submit the original of this document to Assistant Superintendent for Curriculum and Instruction, as appropriate, by September 10 of each school year.

Original: Assistant Superintendent for Curriculum and Instruction
Copy to: Chief Financial Officer
Campus Principal
Campus PEIMS Administrator

APPROVED: 7/20/15

EXHIBIT B

Northwest Independent School District

Six-Week Grading Period PEIMS Verification

Campus	Grading Period	School Year
	❑ 1st ❑ 3rd ❑ 5th ❑ 2nd ❑ 4th ❑ 6th	

Following the conclusion of each six-week grading period, the Campus PEIMS Administrator and the appropriate PEIMS Data Entry Personnel shall verify the accuracy of the PEIMS data and sign this form acknowledging completion of the verification and accuracy of data.

Data Entry Verification

PEIMS Data Personnel's Signature	Printed Name	Date
	Enrollment Data	
	Attendance Data	
	Bilingual Data	
	ESL Data	
	G/T Data	
	Special Education Data (Speech Path.)	
	Special Education Data (Diagnostician)	
	Title I Data	
	At-Risk Data	
	Pregnancy Program Data	
	Discipline Data	
	Discipline Data	
	Discipline Data	
	Discipline Data	
	Discipline Data	
	Discipline Data	
	Discipline Data	
	Other Data: _____	
	Other Data: _____	

Campus PEIMS Administrator's Verification

Campus PEIMS Administrator (Print)	Campus PEIMS Administrator's Signature	Date

Please submit the original of this document to the Assistant Superintendent for Curriculum and Instruction by the end of the third week following the end of a six-week grading period.

Original: Assistant Superintendent for Curriculum and Instruction
Copy to: Chief Financial Officer
Campus Principal
Campus PEIMS Administrator

EXHIBIT C

NORTHWEST INDEPENDENT SCHOOL DISTRICT

STUDENT GUIDELINES FOR ACCEPTABLE USE OF TECHNOLOGY RESOURCES

Acceptable Use for Technology Resources

The Northwest Independent School District ("Northwest ISD", "NISD", or the "District") provides technology resources to its students and staff primarily for educational and administrative purposes. The goal in providing these resources is to promote educational excellence within Northwest ISD by facilitating resource sharing, innovation, and communication with the support and supervision of parents, teachers, and support staff. The use of these technology resources is a privilege, not a right.

With access to many different technology resources and people from all over the world, there comes the potential availability of material that may not be considered to be of educational value in the context of the school setting. Northwest ISD firmly believes that the value of information, interaction, and research capabilities available (including, but not limited to, e-mail, the Internet, and social media) outweighs the possibility that users may obtain material that is not consistent with the educational goals of the District. Access to the District's electronic communication and data management systems, including without limit its telephone system, software, hardware, technology resources, computer networks, electronic mail systems, video conferencing systems, its Internet and Intranet access capabilities, or other technology related systems (collectively referred to herein as the "System") shall be made available to students for education and administrative purposes that are consistent with the goals and mission of the District.

Proper behavior, as it relates to the use of the System, is no different than proper behavior in all other aspects of Northwest ISD activities. All users are expected to use the System in a responsible, ethical, polite manner, and in accordance with NISD Board of Trustees' Policies. This document is intended to clarify those expectations as they apply to technology resource usage and is consistent with District policy.

These guidelines are provided so that students and parents are aware of the responsibilities students accept when they use District-owned computer hardware, operating system software, application software, stored text, data files, electronic mail, local databases, CD-ROMs, digitized information, communication technologies, social media resources, Internet access, electronic communication, and electronic equipment provided by the District. In general, this requires efficient, ethical, and legal utilization of all technology resources.

1. Expectations are as follows:

a. The District's technology resources will be used by students primarily for learning purposes consistent with the District's mission and goals, but some limited personal use is permitted.

b. In a classroom setting, student use of the System is only allowed when supervised or granted permission by a staff member.

c. All users are expected to follow existing copyright laws. Copyright guidelines are posted and/or available in the libraries of each campus as well as posted on the District's Web site.

d. Although the District has an Internet safety plan in place, students are expected to notify a teacher or a campus administrator whenever they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.

e. Students who identify or know about a security problem are expected to convey the details to their teacher or a campus administrator without discussing it with other students.

f. Students are responsible for the proper handling and care of technology devices and for returning them in good working conditions.

2. Unacceptable conduct includes, but is not limited to, the following:

a. Using the System for any illegal activities, including copyright, license, or contract violations or downloading inappropriate materials, viruses, and/or software, such as, but not limited to, hacking and host file-sharing software.

b. Possessing, accessing, transmitting, copying, or creating material that violates the *Student Handbook and Student Code of Conduct,* District policy, or District rules and regulations, including but not limited to content that is inappropriate, illegal, copyrighted, pornography or obscene, stolen, threatening, discriminatory, harassing, or offensive.

c. Attempting to bypass or disable the District's Internet filter, security systems, or software.

d. Attempting to access or install unlicensed, inappropriate, or unapproved software or technology.

e. Plagiarizing or using of District technology resources to engage in academic dishonesty.

f. Using the network for financial or commercial gain, advertising, or political lobbying.

g. Accessing or exploring online locations or materials that do not support the curriculum and/or are inappropriate for school assignments, such as, but not limited to, pornographic sites.

h. Vandalizing and/or tampering with the System. Use or possession of hacking software is strictly prohibited.

i. Unauthorized use of the System and/or any District technology resource or personal/NISD device for non-educational purposes or outside the bounds of NISD curriculum.

j. Knowingly causing congestion on the System or interfering with the work of others.

k. Intentionally wasting System resources (i.e., intentionally accessing an online service where the District only has a finite number of hours of use and leaving the computer logged onto the service while no longer using the online service).

l. Gaining unauthorized access anywhere on the System.

m. Revealing the home address or phone number of one's self or another person, unless done upon the prior request of the District.

n. Invading the privacy of other individuals.

o. Using another user's account, password, or ID card or allowing another user to access your account, password, or ID.

p. Coaching, helping, observing, or joining any unauthorized activity on the System.

q. Posting anonymous messages or unlawful information on the System.

r. Engaging in sexual harassment or submitting, publishing, or displaying any inaccurate, racially and/or culturally offensive, sexually offensive, sexually oriented, abusive, obscene, profane, threatening, terroristic, demeaning, stalking, or slanderous messages, whether public or private.

s. Falsifying permission, authorization, or identification documents.

t. Obtaining copies of or modifying files, data, or passwords belonging to other users on the System.

u. Attempting to upload, create, install, or transmit a computer virus, Trojan, or other technology malware on a computer or the System.

v. Using e-mail, the Internet, or social media resources at school to encourage illegal behavior, engage in conduct that is in conflict or violates the *Student Handbook and Student Code of Conduct*, or threaten school safety.

w. Using personal e-mail, the Internet, the System, or social media resources, without regard to whether it occurs on school property, to engage in conduct that involves a public school and contains the elements of the offense of terroristic threat or false alarm, or otherwise causes a substantial disruption to the educational environment.

x. Downloading software on the System or any system connected to the District's System without prior permission from District.

y. Placing any copyrighted software or data on the District's System or any system connected to the District's System without prior permission from the holder of the copyright. Only the copyright owner or individual the owner specifically authorizes may upload copyrighted materials to the System.

3. Acceptable use guidelines for the System's computer online services are as follows:

a. General Guidelines:

(1) Students will have access to all available forms of electronic media and communication that is in support of education and research, and in support of the educational goals and objectives of the District.

(2) Students are responsible for their ethical and educational use of the System.

(3) All policies and restrictions of the System must be followed.

(4) Access to the System is a privilege and not a right. Each student, and/or parent will be required to sign the Student Guidelines Acceptable Use of Technology Resources Agreement and adhere to these Guidelines in order to be granted access to the System.

(5) The use of any District computer online services in the District must be in support of education and research and in support of the educational goals and objectives of the District.

(6) When placing, removing, or restricting access to specific databases or other District computer online services, school officials will apply the same criteria of educational suitability used for other educational resources.

(7) Transmission of any material that is in violation of any federal or state law is prohibited. This includes, but is not limited to, confidential information, copyrighted material, threatening or obscene material, and computer viruses.

(8) Any attempt to alter data, the configuration of a computer, or the files of another user without the consent of the individual, campus administrator, or technology administrator, will be considered an act of vandalism and subject to disciplinary action in accordance with the District's *Student Handbook and Student Code of Conduct* and District policy.

(9) Parents concerned with the District's computer online services at their child's school should refer to EFA(LOCAL): Instructional Resources: Instructional Material Selection and Adoption policy and follow the state procedure.

(10) Parents will assume responsibility for imposing restrictions only on their own children.

b. System Etiquette:

All System users are expected to observe the following System etiquette:

(1) Swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.

(2) Pretending to be someone else when sending/receiving messages is prohibited.

(3) Submitting, publishing, or displaying any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented or threatening materials or messages either public or private is prohibited.

(4) Transmitting obscene messages or pictures is prohibited.

(5) Revealing and/or posting any personally identifiable information such as addresses, phone numbers, or photographs of another individual on any website or social media network, is prohibited unless the student reveals and/or posts such personal information in compliance with all school policies and under the supervision and consent of a teacher and/or administrator. Other restrictions apply to revealing and/or posting personally identifiable information about other students. (see (3) (b) (7) below)

(6) Using the network in such a way that would disrupt the use of the network by other users is prohibited.

(7) Revealing and/or posting any personally identifiable information, including photographs, of another student on any website or social media network, including the District's website, is prohibited unless (a) such information is directory information; (b) the directory information privacy code specified for the student allows it as recorded in eSchool Plus; (c) the release and/or posting of such personal information is in compliance with District policy FL (LEGAL); and (d) the release and/or posting of such personal information is under the supervision of a teacher and/or administrator.

c. Monitored Use and No Right to Privacy:

(1) Electronic mail transmissions and other use of the System by students are not private and may be monitored, reviewed, audited, intercepted, accessed, or disclosed at any time by designated District staff to ensure appropriate use, ensure the safety and integrity of the System, diagnose problems, and investigate reports of illegal or impermissible activities.

(2) Users should be aware that the District will comply with lawful orders of courts, such as subpoenas and search warrants. The District is also subject to the Texas Public Information Act which may require disclosure of information transmitted through its System, including e-mail communications.

d. E-Mail:

(1) E-mail should be used primarily for educational purposes.

(2) E-mail transmissions, stored data, transmitted data, or any other use of the System by students, employees, or any other user shall not be considered confidential and may be monitored at any time by designated staff to ensure appropriate use.

(3) All e-mail and all e-mail content are property of the District.

(4) E-mails should only be forwarded by a student to another person that would need the information contained in the e-mail for educational or administrative purposes that are consistent with the goals and mission of the District.

(5) Never assume electronic mail is private. Messages relating to or in support of illegal activities must be reported to the authorities and the District will comply with state and federal laws, as well as court orders or subpoenas that will require disclosure.

(6) Include your signature (name, position, affiliation, and Internet address) at the bottom of e-mail messages.

(7) Send only to individuals and/or groups you know.

e. Blogs, Podcasts, Social Networking, and Wikis:

(1) Only students or teacher-created blogs or podcasts related to and in support of the District-approved curriculum and in compliance with all District policies may be posted using the System. Use of the System to post personal blogs, forums, wikis, or podcasts is prohibited.

(2) Participation in social networking websites or chat rooms for educational purposes is permissible for students, under the supervision of a District's teacher, librarian, or administrator.

(3) Students participating in social networking websites and chat rooms using District electronic resources should assume that all content shared, including pictures, is public. Students should not respond to requests for personally identifying information or contact unknown individuals. Caution should be taken when addressing questions that would violate FERPA (Family Education Rights and Privacy Act) or student information. No student shall post on a website personally identifiable information, including photographs, of himself/herself or any other student. (See (3) (b) (5) and (3) (b) (7).)

(4) Posting any student or teacher created podcast and/or blog projects that are not directly related to and in support of the NISD approved curriculum is prohibited.

(5) Posting of any unsupervised student blog is prohibited.

f. Display of Student Work or Information:

The following conditions apply to the display of student work including, but not limited to, art work, class work, photographs, podcasts, projects, and writings on the District's websites or other Internet sites. Student work that has been recorded for a grade is considered an "educational record".

(1) All student work or photographs to be displayed must follow the standards for the "Limitations on Content" as sited in NISD Local policies FNAA and GKDA, and when applicable, must be compliant with the dress code as described in the *NISD Student Handbook and Student Code of Conduct*.

(2) Parental consent for students under the age of 18 must be obtained prior to posting student-created work on campus and/or District websites, social networking, and/or other Internet sites. (See (3) (b) (5) and (3) (b) (7).)

(3) Students may not transmit pictures without obtaining prior permission from all individuals depicted, or from parents of depicted individuals who are under the age of 18.

(4) Student photographs and/or student work may only be displayed with directory information for which the directory information privacy code specified for the student allows it as recorded in eSchool Plus.

g. Hyperlinks:

The following requirements must be met to utilize hyperlinks on any District web page. If these conditions are not met, or promotes the violation of any District policy, regulation, or any local, state, or federal regulation or law, immediate disciplinary action of the individual responsible for the content, file, and/or posting of the hyperlink may be recommended.

(1) Hyperlinks to external (non-District) websites must include the following text on the District web page where the hyperlink exists. "Northwest ISD is not responsible for content on external sites or servers."

(2) Hyperlinks to external (non-District) websites are only allowed where the content in those websites support and/or enhance learning, academic knowledge, and/or provide information necessary to provide service to District web patrons. However, if the content in these websites is judged unsuitable at any time, the hyperlink to the site will be removed.

(3) Hyperlinks to websites, whose content is prohibited by the District's web filtering system, will no be allowed.

(4) Hyperlinks to District employee, volunteer, or student personal websites are not allowed.

h. Filtering and Requests to Disable Filter:

The District will use filtering devices or software that blocks Internet access to visual depictions that are obscene, violent, pornographic, inappropriate for students, or harmful to minors as defined by the federal Children's Internet Protection Act and as determined by the Superintendent or designee.

(1) Internet filters may be disabled for employees based on a Tiered Access System.

(2) Employees may request to use a blocked Internet site for research, or other educational or lawful purposes. Students may have the opportunity to view District approved disabled blocked Internet sites under the supervision of a staff member as it relates to the instruction.

(3) Students will not have the authority to request Internet filters to be disabled.

4. Intellectual Property Rights:

A student shall retain all rights to work created as part of instruction or using District technology resources.

5. Reporting Theft or Releasing Resources:

a. Electronic resources owned by the District should not be released to anyone, including but not limited to, law enforcement agencies. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to violations of computer crime laws. Contents of e-mail and network communications are governed by the Texas Public Information Act, therefore; proper authorities will be given access to their content.

b. Report theft or loss to the School Resource Officers (SRO) within 48 hours. If the incident occurs on the weekend or school holiday, a report must be filed upon 48 hours of returning to school. Failure to report the theft or loss will result in the parent or guardian, or a student 18 years or older, being held responsible for the replacement of the technology material/device at fair market value.

6. Consequences of improper use are as follows:

a. The student in whose name a system account and/or computer hardware is issued will be responsible at all times for its appropriate use. Noncompliance with the *Student Guidelines for Acceptable Use of Technology Resources*, the *Student Handbook and Student Code of Conduct*, and Board policy CQ may result in suspension or termination of System privileges and disciplinary actions. This may also require restitution for costs associated with the necessary repairs and/or replacement of system, hardware, or software if any damage was caused by student's noncompliance or improper use of District's System.

b. Use or possession of hacking software is strictly prohibited and violators will be subject to Phase III consequences of the *Student Handbook and Student Code of Conduct*.

c. Violations of applicable state and federal laws, including the Texas Penal Code, Computer Crimes, Chapter 33, will result in criminal prosecution, as well as disciplinary actions by the District.

d. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to violations of computer crime laws. Contents of e-mail and network communications are governed by the Texas Public Information Act; therefore, proper authorities will be given access to their content.

7. Disclaimer:

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied, including without limitation, those of merchantability and fitness for particular purpose with respect to any services provided by the System and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on the System will meet the system user's requirements, or that the System will be uninterrupted or error free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by System users, information providers, service providers, or other third-party individuals in the System are those of the providers and not the District.

The District will cooperate fully with local, state, and federal officials in any investigation concerning or relating to misuse of the District's electronic communications System.

EXHIBIT D

NORTHWEST INDEPENDENT SCHOOL DISTRICT

EMPLOYEE GUIDELINES FOR ACCEPTABLE USE OF TECHNOLOGY RESOURCES

Acceptable Use for Technology Resources

The Northwest Independent School District ("Northwest ISD", "NISD", or the "District") provides technology resources to its students and staff primarily for educational and administrative purposes. The goal in providing these resources is to promote educational excellence within Northwest ISD by facilitating resource sharing, innovation and communication with the support and supervision of parents, teachers, and support staff. The use of these technology resources is a privilege, not a right.

With access to many different technology resources and people from all over the world, there comes the potential availability of material that may not be considered to be of educational value in the context of the school setting. Northwest ISD firmly believes that the value of information, interaction, and research capabilities available (including, but not limited to, e-mail, the Internet, and social media) outweighs the possibility that users may obtain material that is not consistent with the educational goals of the District. Access to the District's electronic communication and data management systems, including without limit its telephone system, software, hardware, technology resources, computer networks, electronic mail systems, video conferencing systems, and its Internet and Intranet access capabilities (collectively referred to herein as the "System") shall be made available to employees for education and administrative purposes that are consistent with the goals and mission of the District.

Proper behavior, as it relates to the use of the System, is no different than proper behavior in all other aspects of Northwest ISD activities. All users are expected to use the System in a responsible, ethical, polite manner, and in accordance with the District's Board Policies. This document is intended to clarify those expectations as they apply to technology resource usage and is consistent with District policy.

These guidelines are provided so that employees are aware of the responsibilities employees accept when they use District-owned computer hardware, operating system software, application software, stored text, data files, electronic mail, local databases, CD-ROMs, digitized information, communication technologies, social media resources, Internet access, electronic communication, and electronic equipment provided by the District. In general, this requires efficient, ethical, and legal utilization of all technology resources.

1. Expectations are as follows:

a. The District's technology resources will be used primarily for learning, teaching, and administrative purposes consistent with the District's mission and goals, but some limited personal use is permitted.

b. The employee shall limit personal electronic communication devices to send or receive calls, text messages, pictures, and videos to breaks, meal times, and before and after scheduled work hours, unless there is an emergency or the use is authorized by a supervisor to conduct district business.

c. All users are expected to follow existing copyright laws. Copyright guidelines are posted and/or available in the libraries of each campus as well as posted on the District's website.

d. Although the District has an Internet safety plan in place, employees are expected to notify their supervisor or the Assistant Superintendent for Curriculum and Instruction or designee whenever

they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.

e. Employees who identify or know about a security problem are expected to convey the details to their supervisor or the Chief Technology Officer or designee without discussing it with others.

f. Employees are responsible for securing technology devices when not in use and for returning them in good working conditions.

g. District employees are considered public servants. The online presence of employees should not be in conflict with Board policies or the District's Acceptable Use Guidelines for Technology Resources.

2. Unacceptable conduct includes, but is not limited to, the following:

a. Use of the System for a purpose other than for learning, teaching, and/or administrative purposes consistent with the District's mission and goals or not in accordance with CQ legal and local policy.

b. Using the System for illegal activities, including copyright, license, or contract violations or downloading inappropriate materials, viruses, and/or software, such as, but not limited to, hacking and host file-sharing software.

c. Using the System for financial or commercial gain, advertising, or political lobbying.

d. Attempting to bypass or disable the District's Internet filter, security systems or software.

e. Attempting to access or install unlicensed, inappropriate, or unapproved software or technology.

f. Plagiarizing or using District technology resources to engage in academic dishonesty.

g. Accessing or exploring online locations or materials that do not support the curriculum and/or are inappropriate for school assignments, such as, but not limited to, pornographic sites.

h. Vandalizing and/or tampering with equipment, programs, files, software, System performance, or other components of the System. Use or possession of hacking software is strictly prohibited.

i. Causing congestion on the System or interfering with the work of others, e.g., chain letters or broadcast messages to lists or individuals.

j. Intentionally wasting System resources (i.e., intentionally accessing an online service where the District only has a finite number of hours of use and leaving the computer logged onto the service while no longer using the online service).

k. Gaining unauthorized access anywhere on the System.

l. Revealing the home address or phone number of another person, unless done upon the prior request of the District.

m. Invading the privacy of other individuals.

n. Using another user's account, password, or ID card or allowing another user to access your account, password, or ID.

o. Coaching, helping, observing, or joining any unauthorized activity on the System.

p. Posting anonymous messages or unlawful information on the System.

q. Engaging in sexual harassment or submitting, publishing, or displaying any inaccurate, racially and/or culturally offensive, sexually offensive, sexually oriented, abusive, obscene, profane, threatening, terroristic, demeaning, stalking, or slanderous messages, whether public or private.

r. Falsifying permission, authorization, or identification documents.

s. Obtaining copies of or modifying files, data, or passwords belonging to other users on the System.

t. Attempting to upload, create, or transmit a computer virus on a computer and/or the System.

u. Using e-mail, the Internet, or social media resources at school to encourage illegal behavior, engage in conduct violates the *Educator Code or Ethics* (NISD Local Policy DH and Exhibit DH), or threaten school safety.

v. Using personal e-mail, the Internet, or social media resources, without regard to whether it occurs on school property, to engage in conduct that involves a public school and contains the elements of the offense of terroristic threat or false alarm, or otherwise causes a substantial disruption to the educational environment.

w. Placing any copyrighted software or data on the System or any system connected to the District's System without prior permission from the holder of the copyright. Only the copyright owner or individual the owner specifically authorizes may upload copyrighted materials to the System.

x. Knowingly communicate with students through a personal social network system in violation of the NISD employee handbook, administrative regulations, *Educator Code or Ethics* (NISD Local Policy DH and Exhibit DH) and CQ legal and local policy.

3. Acceptable use guidelines for the System's computer online services are as follows:

a. General Guidelines:

(1) Employees will have access to all available forms of electronic media and communication that is in support of learning, teaching, and/or administration, and in support of the educational goals and objectives of the District.

(2) Employees are responsible for their ethical and educational use of the System in the District.

(3) All policies and restrictions of the System must be followed.

(4) Access to the System is a privilege and not a right. Each employee, will be required to sign the *Employee Guidelines Acceptable Use of Technology Resources Agreement* and adhere to these guidelines in order to be granted access to the System.

(5) The use of System must be in support of education and research and in support of the educational goals of the District in accordance with CQ legal and local policy.

(6) When placing, removing, or restricting access to specific databases or other computer

online services, school officials will apply the same criteria of educational suitability used for other educational resources.

(7) Transmission of any material that is in violation of any federal or state law is prohibited. This includes, but is not limited to, confidential information, copyrighted material, threatening or obscene material, and computer viruses.

(8) Any attempt to alter data, the configuration of a computer, or the files of another user without the consent of the individual, campus administrator, or technology administrator, will be considered an act of vandalism and subject to disciplinary action in accordance with the District's Board Policy.

(9) Employees must purge electronic mail and data files in accordance with the District's established retention guidelines.

a. System Etiquette:

All System users are expected to observe the following System etiquette:

(1) Swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.

(2) Pretending to be someone else when sending/receiving messages is prohibited.

(3) Submitting, publishing, or displaying any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented or threatening materials or messages, whether public or private, is prohibited.

(4) Transmitting obscene messages or pictures is prohibited.

(5) Revealing and/or posting any personally identifiable information such as addresses, phone numbers, or photographs of another individual on any website or social media network, is prohibited unless the employee reveals and/or posts such personal information in compliance with all school policies. Other restrictions apply to revealing and/or posting personally identifiable information about students. (See (3) (b) (7) below.)

(6) Using the network in such a way that would disrupt the use of the System by other users is prohibited.

(7) Revealing and/or posting any personally identifiable information, including photographs, of any student on any website or social media network, including the District's website, is prohibited unless (a) such information is directory information, (b) the directory information privacy code specified for the student allows it as recorded in eSchool Plus, (c) the release and/or posting of such personal information is in compliance with District Policy FL (LEGAL).

b. Monitored Use and No Right to Privacy:

a. Electronic mail transmissions and other use of the System by employees are not private and may be monitored, reviewed, audited, intercepted, accessed, or disclosed at any time by designated District staff to ensure appropriate use, ensure the safety and integrity of the System, diagnose problems, and investigate reports of illegal or impermissible activities.

b. Users should be aware that the District will comply with lawful orders of courts, such as subpoenas and search warrants. The District is also subject to the Texas Public Information Act which may require disclosure of information transmitted through its System, including e-mail communications.

c. E-Mail:

(1) E-mail should be used primarily for educational and administrative purposes.

(2) E-mail transmissions, stored data, transmitted data, or any other use of the System by employees or any other user shall not be considered confidential and may be monitored at any time by designated staff to ensure appropriate use.

(3) All e-mail and all e-mail contents are property of the District.

(4) E-mails may only be forwarded by an employee only if such e-mail is forwarded to a person who would need the information contained in the e-mail for educational or administrative purposes that are consistent with the goals and mission of the District.

(5) Never assume electronic mail is private. Messages relating to or in support of illegal activities must be reported to the authorities and the District will comply with state and federal laws, as well as court orders or subpoenas that will require disclosure.

(6) An employee must include his/her signature (name, position, affiliation, and Internet address) at the bottom of e-mail messages.

d. Blogs, Podcasts, Social Networking, and Wikis:

(1) Only students or teacher-created blogs or podcasts related to and in support of the District-approved curriculum and in compliance with all District policies may be posted using the System. Use of the System to post personal blogs, forums, wikis, or podcasts must be in accordance with CQ legal and local policy.

(2) Participation in social networking websites or chat rooms for educational and administrative purposes is permissible for employees and those students under the supervision of a District teacher, librarian, or administrator.

(3) Employees participating in social networking websites and chat rooms using District electronic resources should assume that all content shared, including pictures, is public. Employees should not respond to requests for personally identifying information or contact unknown individuals. Caution should be taken when addressing questions that would violate FERPA (Family Education Rights and Privacy Act) or student information. No employee shall post personally identifiable information, including photographs, of a student on any website, including the District's website without parental consent. (See (3) (b) (5) and (3) (b) (7).)

(4) Posting any student- or teacher-created podcast and/or blog projects that are not in support of the NISD vision, mission, and goals is prohibited.

(5) Posting of any unsupervised student blog is prohibited.

e. Display of Student Work or Information:

The following conditions apply to the display of student work including, but not limited to, art work, class work, photographs, podcasts, projects, and writings on the District's websites or other Internet sites. Student work that has been recorded for a grade is considered an "educational record".

(1) All student work or photographs to be displayed must follow the standards for the "Limitations on Content" as sited in NISD Local policies FNAA and GKDA, and when applicable, is compliant with the dress code as described in the *NISD Student Handbook and Student Code of Conduct*.

(2) Parental consent for students under the age of 18 must be obtained prior to posting student-created work on campus and/or District websites, social networking and/or other Internet sites. (See (3) (b) (5) and (3) (b) (7).)

(3) Employees may not transmit pictures without obtaining prior permission from all individuals depicted, or from parents of depicted individuals who are under the age of 18.

(4) Student photographs and/or student work may only be displayed with directory information for which the directory information privacy code specified for the student allow it as recorded in eSchool Plus.

g. Hyperlinks:

The following requirements must be met to utilize hyperlinks on any District web page. If these conditions are not met, or promotes the violation of any District policy, regulation, or any local, state, or federal regulation or law, immediate disciplinary action of the individual responsible for the content, file, and/or posting of the hyperlink may be recommended.

(1) Hyperlinks to external (non-District) websites must include the following text on the District web page where the hyperlink exists. "Northwest ISD is not responsible for content on external sites or servers."

(2) Hyperlinks to external (non-District) websites are only allowed where the content in those websites support and/or enhance learning, academic knowledge, and/or provide information necessary to provide service to District web patrons. However, if the content in these websites is judged unsuitable at any time, the hyperlink to the site will be removed.

(3) Hyperlinks to websites, whose content is prohibited by the District's web filtering System, will no be allowed.

(4) Hyperlinks to District employee, volunteer, or student personal websites are not allowed.

h. Filtering and Requests to Disable Filter:

The District will use filtering devices or software that blocks Internet access to visual depictions that are obscene, violent, pornographic, inappropriate for students, or harmful to minors as defined by the federal Children's Internet Protection Act and as determined by the Superintendent or designee.

(1) Internet filtering may be disabled for employees based on a Tiered Access System that is available on the District's website.

(2) Employees may request to use a blocked site for research, or other educational or lawful purposes. The request must be filed with and approved by the Chief Technology Officer or designee.

4. Intellectual Property Rights:

a. The District will own any work or work product created by an employee using the System, including a student employee, if it is in the course and scope of the employee's employment, including the right to obtain copyrights.

.

b. The District will retain the right to use any product created in the scope of a person's employment even when the author is no longer an employee of the District.

c. An employee who obtains a patent for such work shall grant a non-exclusive, non-transferable, perpetual, royalty-free District-wide license to the District for use of the patented work.

d. A student will retain all rights to work created as part of instruction or using District technology resources.

5. Reporting Theft or Releasing Resources:

a. Electronic resources owned by the District should not be released to anyone, including but not limited to, law enforcement agencies.

b. Report theft or loss to the District's Personnel and Risk Management Office within 48 hours, if possible. If the incident occurs on the weekend or school holiday, please attempt to report the theft or loss upon 48 hours of returning to school. A copy of the police report should accompany the theft or loss claim.

6. Consequences of improper use are as follows:

a. The employee in whose name a system account and/or computer hardware is issued will be responsible at all times for its appropriate use.

b. Noncompliance with the *Employee Guidelines for Acceptable Use of Technology Resources* and in Board policy CQ may result in suspension or termination of System privileges and disciplinary actions. Violations of applicable state and federal law, including the Texas Penal Code, Computer Crimes, and Chapter 33 will result in criminal prosecution, as well as disciplinary actions by the District. This may also require restitution for costs associated with the necessary repairs and/or replacement of system, hardware, or software if any damage was caused by noncompliance.

c. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to violations of computer crime laws. Contents of e-mail and network communications are governed by the Texas Public Information Act; therefore, proper authorities will be given access to their content.

7. Disclaimer:

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied, including without limitation, those of merchantability and fitness for particular purpose with respect to any services provided by the System and any information contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on the System will meet the System user's requirements, or that the System will be uninterrupted or error free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by System users, information providers, service providers, or other third-party individuals in the System are those of the providers and not the District.

The District will cooperate fully with local, state, and federal officials in any investigation concerning or relating to misuse of the District's electronic communications System.

EXHIBIT D

NORTHWEST ISD EMPLOYEE GUIDELINES FOR ACCEPTABLE USE OF TECHNOLOGY RESOURCES AGREEMENT

Employee Name *(print)* _____

School/Location _____

I have read, understand, and will comply with the Employee Guidelines for Acceptable Use for Technology Resources for Northwest ISD (Employee "AUP"). I further understand that electronic mail transmissions and other use of the electronic communications systems, including the Internet are not private and may be monitored at any time by the District staff to ensure appropriate use, as defined by the *Employee Guidelines for Acceptable Use of Technology Resources*. I understand that noncompliance with the Employee AUP may result in suspension of my access or termination of my privileges and other disciplinary action (including change of employment status, appropriate legal action, and/or termination of employment) consistent with Board Policies and state law. I realize that any of my actions that may violate the law may result in criminal prosecution as well as disciplinary action by the District. Any violation of the *Employee Guidelines for Acceptable Use of Technology Resources* that results in System disruption or damage may result in the assignment of financial liability to me.

Employee Signature _____**Date** _____

PLEASE SIGN THIS FORM AND TURN IT IN TO YOUR CAMPUS ADMINISTRATOR OR DEPARTMENTAL SUPERVISOR.

EXHIBIT E

NORTHWEST INDEPENDENT SCHOOL DISTRICT

BOARD MEMBER GUIDELINES FOR ACCEPTABLE USE OF TECHNOLOGY RESOURCES

Acceptable Use for Technology Resources

The Northwest Independent School District ("Northwest ISD", "NISD", or the "District") provides technology resources to its board members primarily for official duties and limited personal use. The goal in providing these resources is to promote educational excellence within Northwest ISD by facilitating resource sharing, innovation and communication with the support and supervision of parents, teachers, and support staff. The use of these technology resources is a privilege, not a right.

With access to many different technology resources and people from all over the world, there comes the potential availability of material that may not be considered to be of educational value in the context of the school setting. Northwest ISD firmly believes that the value of information, interaction, and research capabilities available (including, but not limited to, e-mail, the Internet, and social media) outweighs the possibility that users may obtain material that is not consistent with the educational goals of the District. Access to the District's electronic communication and data management systems, including without limit its telephone system, software, hardware, technology resources, computer networks, electronic mail systems, video conferencing systems, and its Internet and Intranet access capabilities (collectively referred to herein as the "System") shall be made available to board members for official duties that are consistent with the goals and mission of the District.

Proper behavior, as it relates to the use of the System, is no different than proper behavior in all other aspects of Northwest ISD activities. All users are expected to use the System in a responsible, ethical, polite manner, and in accordance with the District's Board Policies. [See policies BBI and CQ] This document is intended to clarify those expectations as they apply to technology resource usage and is consistent with board policy and administrative regulations.

These guidelines are provided so that board members are aware of the responsibilities the board members accept when they use District-owned computer hardware, operating system software, application software, stored text, data files, electronic mail, local databases, CD-ROMs, digitized information, communication technologies, social media resources, Internet access, electronic communication, and electronic equipment provided by the District. In general, this requires efficient, ethical, and legal utilization of all technology resources.

1. Expectations are as follows:

a. The District's technology resources will be used primarily for official duties, but some limited personal use is permitted.

b. All users are expected to follow existing copyright laws. Copyright guidelines are posted and/or available in the libraries of each campus as well as posted on the District's website.

c. Although the District has an Internet safety plan in place, board members are expected to notify the superintendent or designee whenever they come across information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.

d. Board members who identify or know about a security problem are expected to convey the details to the superintendent or designee without discussing it with others.

e. Board members are responsible for securing technology devices when not in use and for returning them in good working conditions.

f. Board members are considered public servants. The online presence of board members should not be in conflict with Board policies or the District's Acceptable Use Guidelines for Technology Resources.

2. Unacceptable conduct includes, but is not limited to, the following:

a. Using the System for illegal activities, including copyright, license, or contract violations or downloading inappropriate materials, viruses, and/or software, such as, but not limited to, hacking and host file-sharing software.

b. Using the System for financial or commercial gain, advertising, or political lobbying.

c. Attempting to bypass or disable the District's Internet filter, security systems or software. Requests to disable a filtering device should be made to the superintendent.

d. Attempting to access or install unlicensed, inappropriate, or unapproved software or technology.

e. Plagiarizing or using District technology resources to engage in dishonest activities.

f. Accessing or exploring online locations or materials that are of adult nature, such as, but not limited to, pornographic sites.

g. Vandalizing and/or tampering with equipment, programs, files, software, System performance, or other components of the System. Use or possession of hacking software is strictly prohibited.

h. Posting or transmitting pictures of students without obtaining prior permission for all individuals depicted or from parents of depicted student who are under the age of 18.

i. Causing congestion on the System or interfering with the work of others, e.g., chain letters or broadcast messages to lists or individuals.

j. Intentionally wasting finite System resources (i.e., intentionally accessing an online service where the District only has a finite number of hours of use and leaving the computer logged onto the service while no longer using the online service).

k. Gaining unauthorized access anywhere on the System or restricted information or resources.

l. Revealing the home address or phone number of one's self or another person, unless done upon the prior request of the District.

m. Invading the privacy of other individuals.

n. Using another user's account, password, or ID card or allowing another user to access your account, password, or ID.

o. Coaching, helping, observing, or joining any unauthorized activity on the System.

p. Posting anonymous messages or unlawful information on the System.

q. Engaging in sexual harassment or submitting, publishing, or displaying any inaccurate, racially and/or culturally offensive, sexually offensive, sexually oriented, abusive, obscene, profane, threatening, terroristic, demeaning, stalking, or slanderous messages, whether public or private.

r. Falsifying permission, authorization, identification documents, or encrypting communications to avoid security review.

s. Obtaining copies of or modifying files, data, or passwords belonging to other users on the System.

t. Attempting to upload, create, or transmit a computer virus on a computer and/or the System or not taking proper security steps to prevent the equipment or System from becoming vulnerable.

u. Using e-mail, the Internet, or social media resources at school to encourage illegal behavior, engage in conduct violates Board Ethics (Legal Policies BBFA and BBFB), or threaten school safety.

v. Using personal e-mail, the Internet, or social media resources, without regard to whether it occurs on school property, to engage in conduct that involves a public school and contains the elements of the offense of terroristic threat or false alarm, or otherwise causes a substantial disruption to the educational environment.

w. Placing any copyrighted software or data on the System or any system connected to the District's System without prior permission from the holder of the copyright. Only the copyright owner or individual the owner specifically authorizes may upload copyrighted materials to the System.

3. Acceptable use guidelines for the System's computer online services are as follows:

a. General Guidelines:

(1) Board members will have access to all available forms of electronic media and communication that is in support of their official duties and in support of the educational goals and objectives of the District.

(2) Board members are responsible for their ethical and limited personal use of the System in the District.

(3) All policies and restrictions of the System must be followed.

(4) Access to the System is a privilege and not a right. Each board member, will be required to sign the *Board Member Guidelines Acceptable Use of Technology Resources Agreement* and adhere to these guidelines in order to be granted access to the System.

(5) The use of System must be in support of education and research and in support of the educational goals and objectives of the District.

(6) When placing, removing, or restricting access to specific databases or other computer online services, school officials will apply the same criteria of educational suitability used for other educational resources.

(7) Transmission of any material that is in violation of any federal or state law is prohibited. This includes, but is not limited to, confidential information, copyrighted material, threatening or obscene material, and computer viruses.

(8) Board members must comply with the District's record management program, the Texas Open Meeting Act, the Public Information Act, the Family Educational Rights and Privacy Act (FERPA), and campaign laws.

b. System Etiquette:

All System users are expected to observe the following System etiquette:

(1) Swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.

(2) Pretending to be someone else when sending/receiving messages is prohibited.

(3) Submitting, publishing, or displaying any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented or threatening materials or messages, whether public or private, is prohibited.

(4) Transmitting obscene messages or pictures is prohibited.

(5) Revealing and/or posting any personally identifiable information such as addresses, phone numbers, or photographs of another individual on any website or social media network, is prohibited unless the user reveals and/or posts such personal information in compliance with all Board policies. Other restrictions apply to revealing and/or posting personally identifiable information about students. (See (3) (b) (7) below.)

(6) Using the network in such a way that would disrupt the use of the System by other users is prohibited.

(7) Revealing and/or posting any personally identifiable information, including photographs, of any student on any website or social media network, including the District's website, is prohibited unless (a) such information is directory information, (b) the directory information privacy code specified for the student allows it as recorded in eSchool Plus, (c) the release and/or posting of such personal information is in compliance with District Policy FL (LEGAL).

c. Monitored Use and No Right to Privacy:

(1) Electronic mail transmissions and other use of the System by employees are not private and may be monitored, reviewed, audited, intercepted, accessed, or disclosed at any time by designated District staff to ensure appropriate use, ensure the safety and integrity of the System, diagnose problems, and investigate reports of illegal or impermissible activities.

(2) Users should be aware that the District will comply with lawful orders of courts, such as subpoenas and search warrants. The District is also subject to the Texas Public Information Act which may require disclosure of information transmitted through its System, including e-mail communications.

d. E-Mail:

(1) E-mail should be used primarily for conducting official duties and limited personal use.

(2) E-mail transmissions, stored data, transmitted data, or any other use of the System by board members or any other user shall not be considered confidential and may be monitored at any time by designated staff to ensure appropriate use.

(3) All e-mail and all e-mail contents are property of the District.

(4) Never assume electronic mail is private. Messages relating to or in support of illegal activities must be reported to the authorities and the District will comply with state and federal laws, as well as court orders or subpoenas that will require disclosure.

(5) A board member should include his/her signature (name, position, affiliation, and Internet address) at the bottom of e-mail messages.

e. Blogs, Podcasts, Social Networking, and Wikis:

(1) Use of the System to post personal blogs, forums, wikis, or podcasts is prohibited.

(2) Board members participating in social networking websites and chat rooms using District electronic resources should assume that all content shared, including pictures, is public. No personally identifying information should be published. Board members should not respond to requests for personally identifying information or contact unknown individuals. Caution should be taken when addressing questions that would violate FERPA (Family Education Rights and Privacy Act) or student information. No board member shall post personally identifiable information, including photographs, of a student on any website, including the District's website. (See (3) (b) (5) and (3) (b) (7).)

(3) Posting any student- or teacher-created podcast and/or blog projects that are not directly related to and in support of the NISD-approved curriculum is prohibited.

(4) Posting of any unsupervised student blog is prohibited.

f. Display of Student Work or Information:

The following conditions apply to the display of student work including, but not limited to, art work, class work, photographs, podcasts, projects, and writings on the District's websites or other Internet sites. Student work that has been recorded for a grade is considered an "educational record".

(1) All student work or photographs to be displayed must follow the standards for the "Limitations on Content" as sited in NISD Local policies FNAA and GKDA, and when applicable, is compliant with the dress code as described in the *NISD Student Handbook and Student Code of Conduct*.

(2) Parental consent for students under the age of 18 must be obtained prior to posting student-created work on campus and/or District websites, social networking and/or other Internet sites. (See (3) (b) (5) and (3) (b) (7).)

(3) Employees may not transmit pictures without obtaining prior permission from all individuals depicted, or from parents of depicted individuals who are under the age of 18.

(4) Student photographs and/or student work may only be displayed with directory information for which the directory information privacy code specified for the student allow it as

recorded in eSchool Plus.

g. Hyperlinks:

The following requirements must be met to utilize hyperlinks on any District web page. If these conditions are not met, or promotes the violation of any District policy, regulation, or any local, state, or federal regulation or law, immediate disciplinary action of the individual responsible for the content, file, and/or posting of the hyperlink may be recommended.

(1) Hyperlinks to external (non-District) websites must include the following text on the District web page where the hyperlink exists. "Northwest ISD is not responsible for content on external sites or servers."

(2) Hyperlinks to external (non-District) websites are only allowed where the content in those websites support and/or enhance learning, academic knowledge, and/or provide information necessary to provide service to District web patrons. However, if the content in these websites is judged unsuitable at any time, the hyperlink to the site will be removed.

(3) Hyperlinks to websites, whose content is prohibited by the District's web filtering System, will no be allowed.

(4) Hyperlinks to District board member, employee, volunteer, or student personal websites are not allowed.

h. Filtering and Requests to Disable Filter:

The District will use filtering devices or software that blocks Internet access to visual depictions that are obscene, violent, pornographic, inappropriate for students, or harmful to minors as defined by the federal Children's Internet Protection Act and as determined by the Superintendent or designee.

(1) Internet filtering may be disabled for board members based on a Tiered Access System that is available on the District's website.

(2) Board members may request to use a blocked site for research, official duties, or lawful purposes. The request must be filed with the superintendent or designee.

i. Intellectual Property Rights:

(1) Board members shall have limited rights to work they create using the System.

(2) The District will retain the right to use any product created in the scope of a board member's official duty even when the author is no longer a board member of the District.

4. Reporting Theft or Releasing Resources:

a. Electronic resources owned by the District should not be released to anyone, including but not limited to, law enforcement agencies.

b. Report theft or loss to the District's Personnel and Risk Management Office within 48 hours, if possible. If the incident occurs on the weekend or school holiday, please attempt to report the theft or loss upon 48 hours of returning to school. A copy of the police report should accompany the theft or loss claim.

5. Consequences of improper use are as follows:

a. The board member in whose name a system account and/or computer hardware is issued will be responsible at all times for its appropriate use.

b. Noncompliance with the *Board Member Guidelines for Acceptable Use of Technology Resources* and Board policies BBI and CQ may result in suspension or termination of System privileges and disciplinary actions. Violations of applicable state and federal law, including the Texas Penal Code, Computer Crimes, and Chapter 33 will result in criminal prosecution. This may also require restitution for costs associated with the necessary repairs and/or replacement of System, hardware, or software if any damage was caused by noncompliance.

c. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to violations of computer crime laws. Contents of e-mail and network communications are governed by the Texas Public Information Act; therefore, proper authorities will be given access to their content.

6. Disclaimer:

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied, including without limitation, those of merchantability and fitness for particular purpose with respect to any services provided by the System and any information contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on the System will meet the System user's requirements, or that the System will be uninterrupted or error free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by System users, information providers, service providers, or other third-party individuals in the System are those of the providers and not the District.

The District will cooperate fully with local, state, and federal officials in any investigation concerning or relating to misuse of the District's electronic communications System.

EXHIBIT E

NORTHWEST ISD
BOARD MEMBER GUIDELINES FOR ACCEPTABLE USE OF TECHNOLOGY RESOURCES AGREEMENT

Board Member's Name *(print)* _____

I have read, understand, and will comply with the *Board Member Guidelines for Acceptable Use for Technology Resources* for Northwest ISD (Board Member "AUP"). I further understand that electronic mail transmissions and other use of the electronic communications systems, including the Internet are not private and may be monitored at any time by the District staff to ensure appropriate use, as defined by the *Board Member Guidelines for Acceptable Use of Technology Resources*.

I understand that noncompliance with the Board Member AUP may result in suspension of my access or termination of my privileges and appropriate legal action consistent with Board policies and state law. I realize that any of my actions that may violate the law may result in criminal prosecution. Any violation of the *Board Member Guidelines for Acceptable Use of Technology Resources* that results in System disruption or damage may result in the assignment of financial liability to me.

In consideration for the privilege to using the District's technology resources, I hereby release the District, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my use of, or inability to use, these resources, including with limitation, the type of damages identified in the District's policy and administrative regulations.

Board Member's Signature _____**Date**_____

Home Address _____

Home Phone _____ **Cell Phone** _____

THE BOARD MEMBER AGREEMENT MUST BE RENEWED EACH SCHOOL YEAR.

PLEASE SIGN THIS FORM AND TURN IT IN TO THE SUPERINTENDENT.

EXHIBIT F

Northwest ISD
Required Signature Page for Elementary School Students
(_____)

Insert School Year

After reviewing the *Verification of Receipt for the Student Handbook and Code of Conduct*, please initial, complete the fields at the bottom of the page, sign, and return this form to your student's school.

_____
parent initials

My signature below signifies that I am aware the *Student Handbook and Code of Conduct* (including the Extracurricular/Co-curricular Student Pledge of Conduct) is available online for my review, including the Student Guidelines for Acceptable Use of Technology Resources, (or I have requested a printed booklet in writing from the campus) and I agree to keep the school informed of changes to my home address and phone numbers.

_____ _____
Student Signature Date

_____
parent initials

I acknowledge that by giving my email address below that I consent to receiving email about my child and school-related activities. By agreeing to use email communication, I release the District, and its trustees, officials, agents, servants, or employees from any and all claims, demands, causes of action for monetary, legal, or equitable relief and damages of any nature arising from the use of, failure to use, or inability to use, the electronic communications system. To initiate communication via electronic mail, please provide your email addresses below.

Student's Legal Name (Last) (First) (Middle)		
Address		
Primary Phone (used for immediate notification)	Campus	Grade
Name of Mother/Guardian (Please Print)	Name of Father/Guardian (Please Print)	
Mother/Guardian Primary Phone	Mother/Guardian Alternate Phone 1	Mother/Guardian Alternate Phone 2
Father/Guardian Primary Phone	Father/Guardian Alternative Phone 1	Father/Guardian Alternate Phone 2
Email Addresses, as applicable (Please Print)		
Mother/Guardian's Primary Email Address:		
Father/Guardian's Primary Email Address:		

Signature of Parent/Guardian	Date

EXHIBIT F

Northwest ISD
Required Signature Page for Elementary Students
(_____)
Insert School Year

Student Guidelines for Acceptable Use of Technology Resources

I agree to follow the rules and abide by the *Student Guidelines for Acceptable Use of Technology Resources*. I understand if I violate any part of the *Guidelines* I will lose my access privilege to any and all of Northwest ISD's network computer online services and technology resources, and I may face disciplinary action. I take responsibility for knowing the contents of the *Student Guidelines for Acceptable Use of Technology Resources*, which is available online in the *Student Handbook and Code of Conduct*, or in print version by request.

Signature of Student	Date

_____
parent initials

My signature below signifies that I am aware the *Student Guidelines for Acceptable Use of Technology Resources* is included in the *Student Handbook and Code of Conduct,* and is available online for my review, or I have requested a printed booklet in writing from the campus.

_____
parent initials

I understand that the Internet is a world-wide group of hundreds of thousands of computer networks. I agree that Northwest ISD does not control the content of these Internet networks or sites. I understand that if my child violates the *Student Guidelines for Acceptable Use of Technology Resources*, his or her access privilege to Northwest ISD's network or technology resources may be revoked and may be subject to disciplinary action. I understand that my child will maintain this privilege as long as procedures described in the *Student Guidelines for Acceptable Use of Technology Resources* are followed.

_____
parent initials

I also grant permission for examples of my child's schoolwork to be published in campus or district publications and/or on the Internet/World Wide Web as an extension of classroom studies, provided that the home address and home phone number are not included. I understand that if I do not want my child to have their schoolwork published on the Web, that I must submit this request in writing annually to my child's principal.

Signature of Parent/Guardian	Date

EXHIBIT G

Northwest ISD
Required Signature Page for Secondary Students
(_____)

Insert School Year

After reviewing the *Verification of Receipt for the Student Handbook and Code of Conduct*, please initial, complete the fields at the bottom of the page, sign, and return this form to your student's school.

_____
Parent initials

My signature below signifies that I am aware the *Student Handbook and Code of Conduct* (including the Extracurricular/Co-curricular Student Pledge of Conduct) is available online for my review, including the Student Guidelines for Acceptable Use of Technology Resources, (or I have requested a printed booklet in writing from the campus) and I agree to keep the school informed of changes to my home address and phone numbers.

_____ _____
Student Signature Date

_____
Parent initials

I acknowledge that by giving my email address below that I consent to receiving email about my child and school-related activities. By agreeing to use email communication, I release the District, and its trustees, officials, agents, servants, or employees from any and all claims, demands, causes of action for monetary, legal, or equitable relief and damages of any nature arising from the use of, failure to use, or inability to use, the electronic communications system. To initiate communication via electronic mail, please provide your email addresses below.

Student's Legal Name (Last) (First) (Middle)		
Address		
Student Home Phone	Campus	Grade
Name of Mother/Guardian (Please Print)	Name of Father/Guardian (Please Print)	
Mother/Guardian Primary Phone	Mother/Guardian Alternative Phone 1	Mother/Guardian Alternative Phone 2
Father/Guardian Primary Phone	Father/Guardian Alternative Phone 1	Father/Guardian Alternative Phone 2
Email Addresses, as applicable (Please Print)		
Mother/Guardian's Primary Email Address:		
Father/Guardian's Primary Email Address:		

Signature of Parent/Guardian	Date

EXHIBIT G

Northwest ISD
Required Signature Page for Secondary Students
(_____)
(Insert School Year)

Student Guidelines for Acceptable Use of Technology Resources

I agree to follow the rules and abide by the *Student Guidelines for Acceptable Use of Technology Resources*. I understand if I violate any part of the *Guidelines* I will lose my access privilege to any and all of Northwest ISD's network computer online services and technology resources, and I may face disciplinary action. I take responsibility for knowing the contents of the *Student Guidelines for Acceptable Use of Technology Resources*, which is available online in the *Student Handbook and Code of Conduct*, or in print version by request.

Signature of Student	Date

_____
parent initials

My signature below signifies that I am aware the *Student Guidelines for Acceptable Use of Technology Resources* is included in the *Student Handbook and Code of Conduct,* and is available online for my review, or I have requested a printed booklet in writing from the campus.

_____
parent initials

I understand that the Internet is a world-wide group of hundreds of thousands of computer networks. I agree that Northwest ISD does not control the content of these Internet networks or sites. I understand that if my child violates the *Student Guidelines for Acceptable Use of Technology Resources*, his or her access privilege to Northwest ISD's network or technology resources may be revoked and may be subject to disciplinary action. I understand that my child will maintain this privilege as long as procedures described in the *Student Guidelines for Acceptable Use of Technology Resources* are followed.

_____
parent initials

I also grant permission for examples of my child's schoolwork to be published in campus or district publications and/or on the Internet/World Wide Web as an extension of classroom studies, provided that the home address and home phone number are not included. I understand that if I do not want my child to have their schoolwork published on the Web, that I must submit this request in writing annually to my child's principal.

Signature of Parent/Guardian	Date