

Olympia C.U.S.D. #16



**SUBSTITUTE TEACHER
PACKET**



OLYMPIA COMMUNITY UNIT SCHOOL DISTRICT #16

Dr. Laura O'Donnell, Superintendent
Mr. Andy Walsh, Assistant Superintendent

Administration Office
903 East 800 North Road
Stanford, IL 61774-9612
Phone: 309-379-6011 Fax: 309-379-2328

Board of Education

Kevin Frazier, President
Carolyn Hansen, Vice President
Steve Matter, Secretary
Doug Maris
Lawn Hohulin
Ann Cross
Gary Springer

District Administration

Dee Salzer- Network
Technology Director
Jan Mullins- Instructional
Technology Director
Scott Thornton- Director of
Maintenance
Dee Gaither - Director of
Transportation
Anna Waters - Food
Services Manager

Building Administration

Olympia High School

Ed Jodkowski, Principal
Mike Jones, Assistant Principal
Mike Castleman, AD
Phone: 309-379-5911
Fax: 309-379-2583

Olympia Middle School

Ben Lee, Principal
Mike Litwiller, Asst. AD
Phone: 309-379-5941
Fax: 309-379-5411

Olympia North Elementary

Matt Hurley, Principal
Phone: 309-963-4514
Fax: 844-367-3062

Olympia South Elementary

Tracey Rogers, Principal
Phone: 217-648-2302
Fax: 217-648-5248

Olympia West Elementary

Mike Castleman, Principal
Phone: 309-392-2671
Fax: 309-392-2497

Dear Substitute Teacher,

Welcome to the Olympia School District. We thank you for your interest in Olympia CUSD #16 and are excited for you to join us in our tradition of excellence!

Before you begin substituting in our District, we do have the following requirements:

- You must apply online on our District website to become a Substitute Teacher.
- You must provide us with a copy of the Substitute Authorization from the Regional Office of Education
- You must complete some District paperwork.

This paperwork will include a final DCFS Background Check, Direct Deposit information (if you choose), State & Federal W4 forms, Employment Verification form & 2 IDs, No Drug & Alcohol Use Agreement, a Mandated Reporter form, and an Internet Agreement form.

If you have any questions about any of these forms or policies, please contact Velma Runyard at the Olympia Administration Office. All completed forms must be returned to Velma Runyard.

We look forward to having you help us *"Empower learners to recognize & achieve personal growth for success."*

Sincerely

Laura O'Donnell

Dr. Laura O'Donnell
Superintendent



OLYMPIA COMMUNITY UNIT SCHOOL DISTRICT #16

Dr. Laura O'Donnell, Superintendent
Mr. Andy Walsh, Assistant Superintendent

Administration Office
903 East 800 North Road
Stanford, IL 61774-9612
Phone: 309-379-6011 Fax: 309-379-2328

Board of Education

Kevin Frazier, President
Carolyn Hansen, Vice President
Steve Matter, Secretary
Doug Maris
Dawn Hohulin
Ann Cross
Gary Springer

Administrative Staff

Debbie Salzer- Network
Technology Director
Janet Mullins- Instructional
Technology Director
Scott Thornton- Director of
Maintenance
Debbie Gaither - Director of
Transportation
Anna Waters - Food
Services Manager

Building Administration

Olympia High School

Ed Jodlowski, Principal
Mike Jones, Assistant Principal
Mike Castleman, AD
Phone: 309-379-5911
Fax: 309-379-2583

Olympia Middle School

Ben Lee, Principal
Mike Litwiller, Asst. AD
Phone: 309-379-5941
Fax: 309-379-5411

Olympia North Elementary

Matt Hurley, Principal
Phone: 309-963-4514
Fax: 844-367-3062

Olympia South Elementary

Debbie Rogers, Principal
Phone: 217-648-2302
Fax: 217-648-5248

Olympia West Elementary

Mike Castleman, Principal
Phone: 309-392-2671
Fax: 309-392-2497

TO: All Employees

FR: Olympia Payroll Department

RE: Direct Deposit

Olympia CUSD #16 requires your net payroll to be deposited directly into your personal checking or savings account. The direct deposit requirement applies to all new staff.

Employees will have their net pay amount credited to their personal depository on or before the 5th and 20th of each month. Direct deposit employees will have access to all payroll information typically provided on a pay stub through the Employee Access portal for Skyward.

There are several guidelines that will apply to the election of the direct deposit option:

1. Any depository which utilizes ACH direct deposit authorization is eligible to be designated by you as your depository of choice. Virtually all banks, savings and loans, and credit unions are in this system. As a precaution, you should verify in advance that the depository indicated on your authorization form has direct deposit capability.
2. You must complete, sign, and return the Authorization Agreement for Automatic Direct Deposits (ACH Credits) form and return it to the Olympia CUSD #16 District Office.
3. The direct deposit system allows us to transmit your entire net paycheck. Employees must choose either a checking or a savings account for the direct deposit destination. Any other arrangements must be made between you and your banking facility.
4. It will be each employee's responsibility to either notify the payroll department in writing of any changes after the initial account has been set up or request a change in bank and/or account number through the Employee Access portal of Skyward. Failure to do so may result in a delay receiving your pay.

If you do not have a checking account, the Hometown Banks location in Minier will provide FREE checking and ATM cards. The bank may be contacted at (309)392-3247.

Please contact the Olympia payroll department at extension 1130 if you have questions or need additional information. Thank you.

AUTHORIZATION AGREEMENT FOR
AUTOMATIC DIRECT DEPOSITS (ACH CREDITS)

I understand that this authorization will remain in effect until the Payroll Department of Olympia C.U.S.D. #16 has received written notification from me of its termination in such time and in such manner as to afford Olympia School District #16 and the depository a reasonable opportunity to act upon it. Under normal circumstances process time is two payroll periods.

Name _____ Social Security number _____
Please Print

Signed _____ Date _____

Select one option

SAVINGS

_____ I have chosen to deposit to my Savings Account. I authorize the Payroll Department of Olympia School District #16 to initiate direct deposit to my Savings account.

Bank Name _____ Branch _____

City _____ State _____ Zip Code _____

Routing Number _____ Account Number _____

CHECKING

_____ I have chosen to deposit to my Checking Account. I authorize the Payroll Department of Olympia School District #16 to initiate direct deposit to my Checking account.

Please attach a Voided Check.

General Personnel

Drug- and Alcohol-Free Workplace; Tobacco Prohibition

All District workplaces are drug- and alcohol-free workplaces. All employees are prohibited from engaging in any of the following activities while on District premises or while performing work for the District:

1. Unlawful manufacture, dispensing, distribution, possession, use, or being under the influence of an illegal or controlled substance.
2. Distribution, consumption, use, possession, or being under the influence of an alcoholic beverage; being present on District premises or while performing work for the District when alcohol consumption is detectable, regardless of when and/or where the use occurred.
3. Possession or use of medical cannabis.

For purposes of this policy a controlled substance means a substance that is:

1. Not legally obtainable,
2. Being used in a manner different than prescribed,
3. Legally obtainable, but has not been legally obtained, or
4. Referenced in federal or State controlled substance acts.

As a condition of employment, each employee shall:

1. Abide by the terms of the Board policy respecting a drug- and alcohol-free workplace; and
2. Notify his or her supervisor of his or her conviction under any criminal drug statute for a violation occurring on the District premises or while performing work for the District, no later than 5 calendar days after such a conviction.

Unless otherwise prohibited by this policy, prescription and over-the-counter medications are not prohibited when taken in standard dosages and/or according to prescriptions from the employee's licensed health care provider, provided that an employee's work performance is not impaired.

To make employees aware of dangers of drug and alcohol abuse, the Superintendent or designee shall perform each of the following:

1. Provide each employee with a copy of this policy.
2. Post notice of this policy in a place where other information for employees is posted.
3. Make available materials from local, State, and national anti-drug and alcohol-abuse organizations.
4. Enlist the aid of community and State agencies with drug and alcohol informational and rehabilitation programs to provide information to District employees.
5. Establish a drug-free awareness program to inform employees about:
 - a. The dangers of drug abuse in the workplace,
 - b. Available drug and alcohol counseling, rehabilitation, re-entry, and any employee assistance programs, and
 - c. The penalties that the District may impose upon employees for violations of this policy.

Tobacco Prohibition

All employees are covered by the conduct prohibitions contained in policy 8:30, *Visitors to and Conduct on School Property*. The prohibition on the use of tobacco products applies both (1) when an employee is on school property, and (2) while an employee is performing work for the District at a school event regardless of the event's location. *Tobacco* shall have the meaning provided in section 10-20.5b of the School Code.

District Action Upon Violation of Policy

An employee who violates this policy may be subject to disciplinary action, including termination. Alternatively, the School Board may require an employee to successfully complete an appropriate drug- or alcohol-abuse rehabilitation program.

The Board shall take disciplinary action with respect to an employee convicted of a drug offense in the workplace within 30 days after receiving notice of the conviction.

Should District employees be engaged in the performance of work under a federal contract or grant, or under a State contract or grant of \$5,000 or more, the Superintendent shall notify the appropriate State or federal agency from which the District receives contract or grant monies of the employee's conviction within 10 days after receiving notice of the conviction.

LEGAL REF.: Americans With Disabilities Act, 42 U.S.C. § 12114.
Compassionate Use of Medical Cannabis Pilot Program, 410 ILCS 130/.
Controlled Substances Act, 21 U.S.C. § 812; 21 C.F.R. § 1308.11 - 1308.15.
Drug-Free Workplace Act of 1988, 41 U.S.C. § 8101 et seq.
Safe and Drug-Free School and Communities Act of 1994, 20 U.S.C. §7101 et seq.
Drug-Free Workplace Act, 30 ILCS 580/.
105 ILCS 5/10-20.5b.

CROSS REF.: 8:30 (Visitors to and Conduct on School Property)

ADOPTED: October 13, 2015

General Personnel

Exhibit – Drug- and Alcohol-Free Workplace - Verification

I have received a copy of the Olympia School District #16 drug and alcohol policy. My signature indicates verification of receipt of the policy.

Signature

Date

DATED: June 1, 2009

General Personnel

Personal Technology and Social Media; Usage and Conduct

Definitions

Includes – Means “includes without limitation” or “includes, but is not limited to.”

Social media – Media for social interaction, using highly accessible communication techniques through the use of web-based and mobile technologies to turn communication into interactive dialogue. This includes *Facebook, LinkedIn, MySpace, Twitter, and YouTube*.

Personal technology – Any device that is not owned or leased by the District or otherwise authorized for District use and: (1) transmits sounds, images, text messages, videos, or electronic information, (2) electronically records, plays, or stores information, or (3) accesses the Internet, or private communication or information networks. This includes, but is not limited to, laptop computers (e.g., laptops, ultrabooks, and chromebooks), tablets (e.g., iPads Kindle, Microsoft Surface, and other Android platform or Windows devices), smartphones (e.g., iPhone, BlackBerry, Android platform phones, and Windows Phone) and other devices (e.g., iPod).

Usage and Conduct

All District employees who use personal technology and social media shall:

1. Adhere to the high standards for appropriate school relationships required by policy 5:120, *Ethics and Conduct* at all times, regardless of the ever-changing social media and personal technology platforms available. This includes District employees posting images or private information about themselves or others in a manner readily accessible to students and other employees that is inappropriate as defined by policy 5:20, *Workplace Harassment Prohibited*; 5:120, *Ethics and Conduct*; 6:235, *Access to Electronic Networks*; 7:20, *Harassment of Students Prohibited*; and the Ill. Code of Educator Ethics, 23 Ill.Admin.Code §22.20.
2. Choose a District-provided or supported method whenever possible to communicate with students and their parents/guardians.
3. Not interfere with or disrupt the educational or working environment, or the delivery of education or educational support services.
4. Comply with policy 5:130, *Responsibilities Concerning Internal Information*. This means that personal technology and social media may not be used to share, publish, or transmit information about or images of students and/or District employees without

proper approval. For District employees, proper approval may include implied consent under the circumstances.

5. Refrain from using the District's logos without permission and follow Board policy 5:170, *Copyright*, and all District copyright compliance procedures.
6. Use personal technology and social media for personal purposes only during non-work times or hours. Any duty-free use must occur during times and places that the use will not interfere with job duties or otherwise be disruptive to the school environment or its operation.
7. Assume all risks associated with the use of personal technology and social media at school or school-sponsored activities, including students' viewing of inappropriate Internet materials through the District employee's personal technology or social media. The Board expressly disclaims any responsibility for imposing content filters, blocking lists, or monitoring of its employees' personal technology and social media.
8. Be subject to remedial and any other appropriate disciplinary action for violations of this policy ranging from prohibiting the employee from possessing or using any personal technology or social media at school to dismissal and/or indemnification of the District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any violation of this policy.

The Superintendent shall:

1. Inform District employees about this policy during the in-service on educator ethics, teacher-student conduct, and school employee-student conduct required by Board policy 5:120, *Ethics and Conduct*.
2. Direct Building Principals to annually:
 - a. Provide their building staff with a copy of this policy.
 - b. Inform their building staff about the importance of maintaining high standards in their school relationships.
 - c. Remind their building staff that those who violate this policy will be subject to remedial and any other appropriate disciplinary action up to and including dismissal.
3. Build awareness of this policy with students, parents, and the community.
4. Ensure that no one for the District, or on its behalf, requests of an employee or applicant access in any manner to his or her social networking website or requests passwords to such sites.
5. Periodically review this policy and any procedures with District employee representatives and electronic network system administrator(s) and present proposed changes to the Board.

LEGAL REF.: 105 ILCS 5/21B-75 and 5/21B-80.
Ill. Human Rights Act, 775 ILCS 5/5A-102.
Code of Ethics for Ill. Educators, 23 Ill.Admin.Code §22.20.
Garcetti v. Ceballos, 547 U.S. 410 (2006).
Pickering v. High School Dist. 205, 391 U.S. 563 (1968).
Mayer v. Monroe County Community School Corp., 474 F.3d 477 (7th Cir. 2007).

CROSS REF.: 5:20 (Workplace Harassment Prohibited), 5:30 (Hiring Process and Criteria), 5:120 (Ethics and Conduct), 5:130 (Responsibilities Concerning Internal Information), 5:150 (Personnel Records), 5:170 (Copyright), 5:200 (Terms and Conditions of Employment and Dismissal), 6:235 (Access to Electronic Networks), 7:20 (Harassment of Students Prohibited), 7:340 (Student Records)

ADOPTED: May 12, 2014

Instruction

Access to Electronic Networks

Electronic networks, including the Internet, are a part of the District's instructional program and serve to promote educational excellence by facilitating resource sharing, innovation, and communication. The Superintendent shall develop an implementation plan for this policy and appoint system administrator(s).

The School District is not responsible for any information that may be lost or damaged, or become unavailable when using the network, or for any information that is retrieved or transmitted via the Internet. Furthermore, the District will not be responsible for any unauthorized charges or fees resulting from access to the Internet.

Curriculum and Appropriate Online Behavior

The use of the District's electronic networks shall: (1) be consistent with the curriculum adopted by the District as well as the varied instructional needs, learning styles, abilities, and developmental levels of the students, and (2) comply with the selection criteria for instructional materials and library resource center materials. As required by federal law and Board policy 6:60, *Curriculum Content*, students will be educated about appropriate online behavior, including but not limited to: (1) interacting with other individuals on social networking websites and in chat rooms, and (2) cyber-bullying awareness and response. Staff members may, consistent with the Superintendent's implementation plan, use the Internet throughout the curriculum.

The District's electronic network is part of the curriculum and is not a public forum for general use.

Acceptable Use

All use of the District's electronic networks must be: (1) in support of education and/or research, and be in furtherance of the goals stated herein or (2) for a legitimate school business purpose. Use is a privilege, not a right. Students and staff members have no expectation of privacy in any material that is stored, transmitted, or received via the District's electronic networks or District computers. General rules for behavior and communications apply when using electronic networks. The District's *Authorization for Electronic Network Access* contains the appropriate uses, ethics, and protocol. Electronic communications and downloaded material, including files deleted from a user's account but not erased, may be monitored or read by school officials.

Internet Safety

Technology protection measures shall be used on each District computer with Internet access. They shall include a filtering device that protects against Internet access by both adults and minors to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by federal law and as determined by the Superintendent or designee. The Superintendent or designee shall enforce the use of such

filtering devices. An administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose, provided the person receives prior permission from the Superintendent or system administrator.

The Superintendent or designee shall include measures in this policy's implementation plan to address the following:

1. Ensure staff supervision of student access to online electronic networks,
2. Restrict student access to inappropriate matter as well as restricting access to harmful materials,
3. Ensure student and staff privacy, safety, and security when using electronic communications,
4. Restrict unauthorized access, including "hacking" and other unlawful activities, and
5. Restrict unauthorized disclosure, use, and dissemination of personal identification information, such as, names and addresses.

Authorization for Electronic Network Access

Each staff member must sign the District's *Authorization for Electronic Network Access* as a condition for using the District's electronic network. Each student and his or her parent(s)/guardian(s) must sign the *Authorization* before being granted unsupervised use. All users of the District's computers to access the Internet shall maintain the confidentiality of student records. Reasonable measures to protect against unreasonable access shall be taken before confidential student information is loaded onto the network. The failure of any student or staff member to follow the terms of the *Authorization for Electronic Network Access*, or this policy, will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

LEGAL REF.: No Child Left Behind Act, 20 U.S.C. §6777.
Children's Internet Protection Act, 47 U.S.C. §254(h) and (i).
Enhancing Education Through Technology Act, 20 U.S.C. §6751
et seq.
47 C.F.R. Part 54, Subpart F, Universal Service Support for
Schools and Libraries.
7:20 ILCS 135/0.01.

CROSS REF.: 5:100 (Staff Development Program), 5:170 (Copyright), 6:40
(Curriculum Development), 6:60 (Curriculum Content), 6:210
(Instructional Materials), 6:230 (Library Media Program), 6:260
(Complaints About Curriculum, Instructional Materials, and
Programs), 7:130 (Student Rights and Responsibilities), 7:190
(Student Discipline), 7:310 (Restrictions on Publications and
Written or Electronic Material)

ADOPTED: July 9, 2012

Acceptable Use Policy for Staff Members

Each staff member must sign this *Acceptable Use Policy* as a condition to being granted use of the District's computer hardware, software, and network including Internet. School Board members, and other individuals provided with network access are treated like staff members for the purposes of this Policy. Please read this carefully before signing.

The purpose of this policy is to provide Olympia staff members with guidance on the proper use of the district's information technology (IT) resources, including but not limited to:

- The Internet, the intranet, email and social networking
- District assigned computing devices
- The district's network and supporting systems and the data transmitted by and stored on these systems

This policy applies to the use of district resources even when off-site. District equipment taken off-site may only be used by district employees. Under no circumstances are non-district persons permitted to use district assigned equipment without formal permission from the district.

All use of the Network/Internet shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. This *Acceptable Use Policy* does not attempt to state all required or prescribed behaviors by users. However, some specific examples are provided. The failure of any user to follow the terms of the *Acceptable Use Policy* will result in the loss of privileges, disciplinary action, and/or appropriate legal action. Users shall be subject to disciplinary action under this policy only after they have been given a copy of this policy. The signature at the end of this document indicates that the party who signed this document has carefully read the terms and conditions of this *Acceptable Use Policy*, understands their significance, and agrees to abide by said terms and conditions.

General Terms and Conditions

1. **Acceptable Use** – Access to the District's computer hardware, software, and network including Internet must be for the purpose of education, communication, or research, and be consistent with the educational objectives of the District as set forth in written Board policy.
2. **Privileges** – The use of the District's information technology resources is a privilege, not a right, and inappropriate use may result in a cancellation of those privileges. The District's Building Principals, in consultation with the District's Technology Director, will make all decisions regarding whether or not a user has violated the *Acceptable Use*

Policy, may deny, revoke or suspend access at any time, and may recommend to the District's Superintendent that discipline be imposed on an employee for a violation of the *Acceptable Use Policy*. If a Building Principal finds an employee to have violated the aforesaid policies and the employee's Network/Internet access is thereby denied, revoked or suspended by the Building Principal, then such employee may appeal the Building Principal's decision to the Superintendent, in writing within five (5) working days of the Building Principal's decision. The Superintendent shall review the matter, may consider additional evidence as the Superintendent deems appropriate, and shall thereafter render a decision in writing. Within five (5) working days after the Superintendent's decision, an employee may request, in writing to the Superintendent, that the Board of Education review the Superintendent's decision. If so requested, the Board of Education will make such review at its next regularly scheduled Board meeting, and shall thereafter render a decision, which shall be final.

3. **Unacceptable Use** – Users of the District information technology resources are responsible for their actions and activities involving the District hardware, software, network and Internet. Examples of unacceptable use include but are not limited to:
- Any illegal activity, including the transmission of any material in violation of any U.S. or State regulation;
 - Infringing the intellectual property rights of others including copyright violation and plagiarism.
 - Transferring out of the district's direct control any software licensed to the district or data owned or licensed to the district without explicit written authorization;
 - Downloading and or installing software unless it is required to complete their job;
 - Revealing confidential or sensitive information, student data, or any other information covered by existing state or federal privacy or confidentiality laws, regulations, rules, policies, procedures, or contract terms;
 - Using the network for commercial gain;
 - Excessive personal use
 - Invading the privacy of individuals;
 - Using another person's account or allowing another person to use a district system under the user's district login or a student login;
 - Posting of anonymous messages;
 - Adding, modifying, repairing, removing, reconfiguring or otherwise tampering with any device on the network infrastructure including but not limited to wireless network devices, workstations, printers, servers, cabling, switches/hubs, routers, etc. Changes to the Olympia information systems must be performed by authorized personnel under the auspices of the Olympia school district
 - Accessing, submitting, posting, publishing or displaying any defamatory, abusive, obscene, profane, pornographic, threatening, racially offensive, politically charged, harassing or illegal materials or material of a sexual nature that is inappropriate in a school environment; and
 - Using the network while access privileges are suspended or revoked.

4. **Limited Personal Use** – occasional and incidental personal use of the District's IT resources and Internet access is allowed subject to limitations. By the allowance of such use, however, the Olympia school district does not grant any ownership, privacy, or expectation of privacy to any person in the contents of any messages or other Internet activities involving Olympia resources or equipment.

Personal use of IT resources is prohibited if:

- It materially interferes with the use of IT resources by the district; or
- Such use burdens the district with additional costs; or
- Such use interferes with the staff member's employment duties or other obligations to the district; or
- Such personal use includes any activity that is prohibited under any district, state or federal statute or policy.

5. **Compliance with copyright laws** – The District intends to adhere to all copyright laws.
6. **No Warranties** – The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages an individual suffers. This includes loss of data resulting from delays, non-deliveries, missed deliveries or service interruptions caused by unforeseen network problems or a user's errors or omissions. Use of any information obtained via the Network/Internet is at a user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.
7. **Telephone Charges** – The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges and/or equipment or line costs.
8. **Unauthorized Access** – Users shall not tamper with the district's security or content filtering safeguards or attempt to gain access to computer data for which the user has no security access. This includes, but is not limited to, financial, employee, or student information. If the security level of a user is in doubt, they are to contact the Technology Director.
9. **Network Etiquette** – Users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:
The User should:
- a. Be Polite; he/she should not become abusive in his/her messages to others.
 - b. Use appropriate language. Individuals should not swear, use vulgarities or any other inappropriate language.
 - c. Not reveal personal information (addresses or telephone numbers, etc. of self or colleagues or students).

- d. Recognize that electronic messages are not private. People who operate the system have access to all email and to other messages. Messages relating to or in support of illegal activities will be reported to the authorities.
 - e. Not use the network in any way that would disrupt its use by other users.
 - f. Consider all communications and information assessable via the network to be the property of the District.
10. **Vandalism** – Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, District hardware, software, the Network/Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.
11. **Security** – Network security is a high priority. Keep your account and password confidential. Users shall not allow another person to use a district system under the user's district login or a student login. Identified security problems on the Network/Internet must only be shared with the Technology Director, Building Principal, or designee. Attempts to log-on to the Internet or Network as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the Network or Internet.
12. **Indemnification** – The user agrees to indemnify the School District for any losses, costs, or damages incurred by the District relating to, or arising out of, any violation of these policies or procedures.
13. **Copyright Web Publishing Rules** – Copyright law and District policy prohibit re-publishing of text or graphics found on the web or on District Web sites or file servers without explicit permission.
- a. For each re-publication on a Web site or file server of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the Web address of the original source.
 - b. Staff engaged in producing Web pages shall only post content for the purpose of education, communication, or research, and that is consistent with the educational objectives of the District as set forth in this policy and any written Board policy.
 - c. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the Web site displaying material may not be considered a source of permission.
 - d. The "fair use" rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.

14. Use of Electronic Mail, Social Networking, and network servers

- a. The District's electronic mail system and its constituent software, hardware, and data files are owned and controlled by the School District. The School District provides e-mail to aid students and staff members in fulfilling their duties and responsibilities, and as an educational tool.
- b. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student or staff member to a network account is strictly prohibited.
- c. Each person should use the same degree of care in drafting electronic mail or social networking messages as would be put into a written memorandum or document. Nothing should be transmitted in any electronic message that would be inappropriate in a letter or memorandum.
- d. Electronic messages transmitted via the School District's Internet gateway carry with them an identification of the user's Internet "domain." This domain name is a registered domain name and identifies the author as being with the School District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of the School District. Users will be held personally responsible for the contents of any and all electronic messages transmitted to external recipients.
- e. Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrator.
- f. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.
- g. Use of School District's electronic mail system and network constitutes consent to these regulations.

15. **Release of Information Outside of the District** - releasing, transporting, electronically transmitting, emailing, or storing sensitive employee or student information outside the physical or logistical control of the district through the use of a USB flash drive or by other means is prohibited without the explicit approval of the District.

16. **Student Supervision** – It is understood that teachers are required to instruct the students on acceptable use of IT equipment, the Network/Internet and on the proper Network/Internet etiquette. It is understood that teachers are responsible for

maintaining appropriate control and supervision of the classroom including student use of District computers and the Network/Internet. It is also understood that employees cannot guarantee appropriate student use of the Network/Internet.

17. **Bringing in Personal Devices** – a staff member who chooses to bring in and use a personal electronic device within the District:

- Must have a signed copy of this AUP on file with the District.
- Accepts that the District bears no responsibility for the security of the personal device.
- Acknowledges that the staff member, and not the District, is responsible for the proper care of his/her personal device including any costs of repair, replacement or any modifications needed to use the device in the District.
- Agrees that, while within the District, the use of his/her personal device will be in compliance with this Acceptable Use Policy and all its guidelines and prohibitions, the same as if the device was issued by the District.

ACKNOWLEDGMENT

Any user who violates the *Acceptable Use Policy* shall be subject to disciplinary action including, but not limited to, revocation of access privileges, written warnings, suspension without pay, or dismissal in accordance with the applicable provisions of Board Policy or the Illinois School Code. Additionally, if a user's conduct constitutes a violation of copyright or other laws, the user may be subject to prosecution under such laws. Any user who intentionally or negligently damages or destroys District hardware and/or software will also be responsible for all costs associated with repair and/or replacement parts and services.

I understand and agree to abide by this *Acceptable Use Policy*.

Employee's Name _____ Date _____
(Please print)

Employee's Signature _____

NOTE: Please sign this acknowledgment the way you want your name printed in the personnel directory and the way you want your e-mail address listed in the Olympia system.

Your e-mail address will be "your.firstname.lastname@olympia.org" as listed in the personnel directory.



OLYMPIA COMMUNITY UNIT SCHOOL DISTRICT #16

Dr. Laura O'Donnell, Superintendent

Mr. Andy Walsh, Assistant Superintendent

Administration Office

903 East 800 North Road

Stanford, IL 61774-9612

SYSTEM ACCESS FOR NEW EMPLOYEES

Once your employment paperwork is returned and processed, you will receive access to the Olympia system. Below are details for accessing the system for the first time.

The logins for Email and Olympia computers are linked. If logging into Email for the first time from home, please choose option #1. If logging into an Olympia computer before accessing Email for the first time, please choose option #2.

OPTION 1

Web Email using the link on the Olympia Home Page:

Login: First Name.Last Name@olympia.org
Temporary Password: Olympia 16**
Domain: oly16.org

**Please see the supplementary instructions for changing your password if you choose the Web Email first option.

District Computer:

Login: First Name.Last Name
Password: Same as Web Email Password

OPTION 2

District Computer

Login: First Name.Last Name
Temporary Password: Olympia16

Outlook Email

Login: First Name.Last Name
Password: Same as District Computer Password

You will be prompted to select a unique password after logging in the first time. Once your password is changed, it will be applied to Outlook mail, Webmail, and the district computer login.

For assistance with access to district computers or Email, please contact the Technology department at (309)379-5911, ext. 9368.

Skyward

Skyward may be accessed using the SkyPort link on the Olympia Home Page or by using the dropdown link on a district computer.

Login: First Name.Last Name***
Temporary Password: Olympia16

***New employees with an existing Family Access login and password will use those same credentials to gain access to the Employee portal.

You will be prompted to select a unique password after logging in the first time.

For assistance with access to Skyward, please contact Human Resources at (309)379-6011, ext. 1130.

Compliance Training (Does not apply to Substitutes)

Access from the Olympia Home Page by navigating to Staff/Compliance Training

Login: First Name.Last Name
Password: Eight Digit Birthdate

For assistance with Compliance Training, please contact the District Office at (309)379-6011, ext. 1127.