PHOENIX-TALENT SCHOOLS

EXCELLENCE for EVERYONE

Technology Use Agreement

Introduction

The Technology Use Agreement/Acceptable Use Agreement (AUP) is intended to prevent online users from unauthorized access and other unlawful or improper activities, prevent unauthorized disclosure of or access to sensitive information, to comply with the Children's Internet Protection Act ("CIPA") and other applicable laws, and establish expectations for use of District systems.

I. **Definitions**

1. As used in this policy, "user" includes anyone using the computers, Internet (including social media, e-mail, and chat rooms), web-based PTS software systems and other forms of direct electronic communications, or equipment provided by the District (the "network.")
2. The Network - The district has established an electronic communications network (network) for electronic communication and access to, and use of, the World Wide Web.
3. Mobile Devices - A mobile device is any portable, electronic device used for communications including telephone, text messaging or data transmissions (eg. email, web-browsing, streaming media, photographs, file transfer, etc.) over any network.

II. **Terms of Permitted Use**

1. Only current students, PTS employees, approved volunteers, school board members and District contractors are authorized to use the network.
2. The District sponsors and owns the network. The network is intended for District-related educational and administrative purposes.
3. By accessing the network, the user acknowledges that they have read and understood the PTS Acceptable Use Policy; the conditions for use remain in effect until:
    i. In case of students, access revoked by the parent, the student loses the privilege of using the District's network, or is no longer a PTS student.
    ii. In case of employees or volunteers, the employee or volunteer loses the privilege of using the District's network or is no longer a PTS employee.
4. All network users are expected to follow this policy and report any misuse of the network to a teacher, administrator, or other appropriate District personnel. Access to the network has been established for educational use only, including support of administrative and student services, student and staff research, lesson planning, collaboration and sharing of ideas, contact with teachers and support staff, and the downloading of materials to be used as educational resources.

5. District employees may use the network for incidental personal use, but this use should be limited and must be in accordance with this AUP, all District policies, administrative directives, and other guidelines regarding computers, networks and Web pages.
6. By using the network, users have agreed to this policy. If a user is uncertain about whether a particular use is acceptable or appropriate, they should consult a teacher, supervisor or other appropriate District personnel.
7. All users authorized to access student information are required to abide by the policies governing review and release of student education records. The Family Educational Rights and Privacy Act (FERPA) of 1974 mandates that information contained in a student's education record must be kept confidential and outlines the procedures for review, release and access to such information. Access to student information systems will be granted only to those individuals who have been determined to have a legitimate educational interest in the data. Individuals who have been granted access must understand and accept all responsibilities of working with confidential student records. In the event of loss of data and/or device, it is the individual's responsibility to immediately notify District administration and follow appropriate established District policy.
8. In order to protect student data and Personally Identifiable Information (PII) the IT Department may implement endpoint protection including encryption on District mobile devices. Individuals who have student data on a mobile device are responsible for the security of that data at all times. It is the responsibility of the primary user of the device to immediately inform the Information Technology Department (IT) in the event of the device being lost, stolen, missing, infected with a virus/malware, hacked, or otherwise compromised. Any mobile device connected to the network or configured to access District email is subject to IT oversight, which may include remotely erasing data on the device at any time.
9. Network users shall have no expectation of personal privacy in the use of the District's network. Passwords are used to protect the security of District data and technologies and are not intended to convey an expectation of personal privacy or exclusion from monitoring.
10. Under the direction of the Superintendent or Assistant Superintendent, the IT Department reserves the right to access and disclose, as appropriate, all information and data stored on District technology, transmitted over the District network and technology. In addition, information and data relevant to any users' work in their District capacity may become discoverable evidence if a public records request is made or for any legal proceedings in which the District may be involved.
11. Authorized District personnel may temporarily suspend or permanently end any user's access.
12. Documents, emails, and other electronic records created, sent or received using the Network are public records and may be subject to disclosure by law. They must be preserved in compliance with District and State record retention and preservation policies. Access to the District's Network from employee-owned computing devices such as employee owned home computers, or any portable computing device (such as a laptop, smartphone, or other electronic device used to access electronic data) may subject the employee's personal devices to disclosure.
13. Employees who participate in an approved PTS Social Media Presence must abide by the rules as defined in Board policy.
14. PTS uses Google Apps for Education for online collaboration with staff and students. Employees using Google Apps for Education must abide by the terms and conditions signed upon initial log-in

to Google Apps for Education, as well as all terms of this policy.

15. PTS employees are required to use district email to conduct all district business, and may not use personal email for any district business.

III. **Prohibited Use**

1. District employees shall not use the network to access obscene material, including pornography, or any other material that is harmful to the district's educational purpose and mission or inconsistent with a professional work environment. If such material is inadvertently accessed, a district employee should notify his or her supervisor as soon as reasonably possible.
2. Violating any state or federal law or municipal ordinance, accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information, or copyrighted materials.
3. Selling or purchasing illegal items or substances.
4. Causing harm to others or damage to their property, such as:
    a. Using profane, abusive, or impolite language; threatening, harassing, bullying or making damaging or false statements about others;
    b. Accessing, transmitting, or downloading offensive, harassing, or disparaging materials;
    c. Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs; or disrupting any computer system performance;
    d. Intentionally causing physical damage to a technology resource; or
    e. Using any device to pursue "hacking," internal or external to the District, or attempting to access or store information protected by privacy laws.
5. Engaging in uses that jeopardize access or lead to unauthorized access into others' accounts or other computer networks, such as:
    a. Attempting to gain unauthorized access to the network or to any other computer system through the network or go beyond your authorized access.
    b. Using another's account password(s) or identifier(s);
    c. Interfering with other users' ability to access their account(s);
    d. Disclosing anyone's password or allowing a person to use another user's account(s);
    e. Providing your account information, including passwords, to others, or making your account readily accessible. Sharing your user credentials with the IT department for troubleshooting purposes is an exception;
    f. Deleting, copying, modifying, or forging other users' names, emails, files, or data; disguising one's identity, impersonating other users, or sending anonymous email; or
    g. Posting or distributing personal information about other District personnel on the District Web site or public Internet without the employee's permission or making any reference to confidential student information on the District Web site or public Internet.
6. Using the network for:

a. Personal financial gain;
b. Personal advertising, promotion, or financial gain;
c. Conducting for-profit business activities and/or engaging in non government related fundraising or public relations activities such as solicitation for religious purposes, lobbying for personal political purposes; or
d. Using software or hardware designed to interfere with or circumvent security mechanisms.
e. Using the network in any manner that violates any District or school rule or policy, including, but not limited to any other rule or policy.

7. Google Apps for Education – PTS uses Google Apps for Education for online collaboration with staff and students. Users agree to not use Google Apps for Education services:
    a. to generate or facilitate unsolicited bulk commercial email;
    b. to violate, or encourage the violation of, the legal rights of others;
    c. for any unlawful, invasive, infringing, defamatory, or fraudulent purpose;
    d. to intentionally distribute viruses, works,Trojan horses, corrupted files, hoaxes, or other items of a destructive nature;
    e. to interfere with the use of the Services, or the equipment used to provide the Services, by customers, authorized resellers, or other authorized users;
    f. to alter, disable, interfere with or circumvent any aspect of the Services;
    g. to test or reverse-engineer the Services in order to find limitations, vulnerabilities or evade filtering capabilities.
8. No user shall establish a peer-to-peer network or wireless ad-hoc using their personal device, or any other wireless device while on district property. This includes, but is not limited to, using a privately-owned electronic device such as a cabled or wireless hotspot.
9. The use of a District account is a privilege, not a right. Misuse could result in the restriction or cancellation of the account. Misuse may also lead to other disciplinary and/or legal action for both students and employees, including suspension, expulsion, dismissal from District employment, or criminal prosecution by government authorities. The District will attempt to tailor any disciplinary action to meet the specific concerns related to each violation. When applicable, sanctions on employees will be in accordance with the appropriate labor agreement.

IV. **Internet Safety**

1. In accordance with the Children's Internet Protection Act (CIPA), the District will use technology protection measures on the network to block or filter, to the extent practicable, access to visual depictions that are obscene, pornographic and/or harmful to minors.
2. Use of the District network constitutes consent to be monitored. Users should have no expectation of privacy regarding their use of District property, network and/or Internet access, files, and other District systems including e-mail. Monitoring technologies may be used to identify and mitigate issues with access to inappropriate materials.
3. It is the intention of Phoenix-Talent Schools to educate our students to be good Cybercitizens. With input from building administrators, teachers, instructional leaders and parents, Information Technology will provide resources and curriculum around topics such as:
    a. Safety and security of minors when using technology such as social networking

websites, email, video games, chat rooms, instant messaging, and other forms of direct electronic communications;

b. Respectful and appropriate online behaviors;
c. Cyberbullying awareness and response;
d. Cyber-ethics awareness including plagiarism, cheating and information literacy.

ESCUELAS DE PHOENIX-TALENT

EXCELENCIA *para* TODOS

Uso aceptable de la política de tecnología del distrito (AUP)

Introducción

La política de uso aceptable del distrito ("AUP") tiene como objetivo evitar que los usuarios en línea tengan acceso no autorizado y otras actividades ilegales o inapropiadas, evitar la divulgación o acceso no autorizado a información confidencial, para cumplir con la Ley de Protección de Niños en Internet ("CIPA") y otras leyes aplicables, y establecer expectativas para el uso de los sistemas del Distrito.

I. **Definiciones**
   A. Tal como se usa en esta política, "usuario" incluye cualquier persona que use las computadoras, Internet (incluidas las redes sociales, el correo electrónico y las salas de chat), los sistemas de software de PTS y otras formas de comunicaciones electrónicas directas o equipos provistos por el Distrito (la "red".)
   B. La red: el distrito ha establecido una red de comunicaciones electrónicas (red) para la comunicación electrónica y el acceso y uso de la World Wide Web.
   C. Dispositivos móviles - Un dispositivo móvil es cualquier dispositivo electrónico portátil utilizado para comunicaciones que incluyen teléfono, mensajes de texto o datos transmisiones (por ejemplo, correo electrónico, navegación web, transmisión de medios, fotografías, transferencia de archivos, etc.) a través de cualquier red.

II. **Condiciones de uso permitido**
   A. Solo los estudiantes actuales, los empleados de PTS, los voluntarios aprobados, los miembros de la junta escolar y los contratistas del Distrito están autorizados a usar la red.
   B. El Distrito patrocina y es dueño de la red. La red está destinada a fines educativos y administrativos relacionados con el Distrito.
   C. Al acceder a la red, el usuario reconoce haber leído y entendido laTPolítica de Uso Aceptable delas condiciones de uso permanecen vigentes hasta que:
      1. En caso de estudiantes, revocadas por los padres, el estudiante pierde el privilegio de usar la red del Distrito, o deja de ser estudiante de PTS.
      2. En caso de empleados o voluntarios, el empleado o voluntario pierde el privilegio de usar la red del Distrito o deja de ser un empleado de PTS.
   D. Se espera que todos los usuarios de la red sigan esta política e informen cualquier uso indebido de la red a un maestro u otro personal apropiado del Distrito. El acceso a la red se ha establecido solo para uso educativo, incluido el apoyo de los servicios administrativos y estudiantiles, la investigación de los estudiantes y el personal, la

planificación de lecciones, la colaboración y el intercambio de ideas, el contacto con los maestros y el personal de apoyo, y la descarga de materiales para ser utilizados como recursos educativos.

E. Los empleados del Distrito pueden usar la red para uso personal incidental, pero este uso debe ser limitado y debe estar de acuerdo con esta AUP, todas las políticas del Distrito, directivas administrativas y otras pautas relacionadas con computadoras, redes y páginas web.
F. Al utilizar la red, los usuarios han aceptado esta política. Si un usuario no está seguro de si un uso en particular es aceptable o apropiado, debe consultar a un maestro, supervisor u otro personal del Distrito apropiado.
G. Todos los usuarios autorizados para acceder a la información de los estudiantes deben cumplir con las políticas que rigen la revisión y divulgación de los registros educativos de los estudiantes. La Ley de privacidad y derechos educativos de la familia (FERPA) de 1974 exige que la información contenida en el registro educativo de un estudiante se mantenga confidencial y describe los procedimientos para revisar, divulgar y acceder a dicha información. El acceso a los sistemas de información de los estudiantes se otorgará solo a aquellas personas que se haya determinado que tienen un interés educativo legítimo en los datos. Las personas a las que se les ha otorgado acceso deben comprender y aceptar todas las responsabilidades de trabajar con expedientes estudiantiles confidenciales. En caso de pérdida de datos y/o dispositivo, es responsabilidad del individuo notificar de inmediato a la administración del Distrito y seguir la política del Distrito apropiada establecida.
H. Para proteger los datos de los estudiantes y la información de identificación personal (PII), el Departamento de TI puede implementar la puntos finales , incluido el cifrado en los dispositivos móviles del Distrito. Las personas que tienen datos de estudiantes en un dispositivo móvil son responsables de la seguridad de esos datos en todo momento. Es responsabilidad del usuario principal del dispositivo informar de inmediato al Departamento de Tecnología de la Información (TI) en caso de pérdida, robo, pérdida, infección del dispositivo con un virus/malware, piratería informática o cualquier otro compromiso. Cualquier dispositivo móvil conectado a la red o configurado para acceder al correo electrónico del Distrito está sujeto a la supervisión de TI, que puede incluir el borrado remoto de datos en el dispositivo en cualquier momento.
I. Los usuarios de la red no deben tener expectativas de privacidad personal en el uso de la red del Distrito. Las contraseñas se utilizan para proteger la seguridad de los datos y las tecnologías del Distrito y no pretenden transmitir una expectativa de privacidad personal o exclusión del monitoreo.
J. Bajo la dirección del Superintendente o Superintendente Auxiliarde Humanos , IT se reserva el derecho de acceder y divulgar, según corresponda, toda la información y los datos almacenados en la tecnología del Distrito, transmitidos a través de la red y la tecnología del Distrito. Además, la información y los datos relevantes para el trabajo de cualquier usuario en su capacidad del Distrito pueden convertirse en pruebas detectables si se realiza una solicitud de registros públicos o para cualquier procedimiento legal en el que el Distrito pueda estar involucrado.

K. El personal autorizado del Distrito puede suspender temporalmente o finalizar permanentemente el acceso de cualquier usuario.
L. Los documentos, correos electrónicos y otros registros electrónicos creados, enviados o recibidos mediante la Red son registros públicos y pueden estar sujetos a divulgación por ley. Deben conservarse de conformidad con las políticas de conservación y retención de registros del Distrito y del Estado. El acceso a la Red del Distrito desde,como computadoras domésticas propiedad de los empleados, o cualquier dispositivo informático portátil (como una computadora portátil, un teléfono inteligente u otro dispositivo electrónico utilizado para acceder a datos electrónicos) puede estar sujeto a la divulgación de los dispositivos personales del empleado.
M. Los empleados que participen en una Presencia de Medios Sociales de PTS aprobada deben cumplir con las reglas definidas en la política de la Junta.
N. PTS utiliza Google Apps for Education para la colaboración en línea con el personal y los estudiantes. Los empleados que utilicen Google Apps for Education deben cumplir con los términos y condiciones firmados al iniciar sesión por primera vez en Google Apps for Education, así como con todos los términos de esta política.
O. PTS deben usar el correo electrónico del distrito para realizar todos los asuntos del distrito y no pueden usar el correo electrónico personal para ningún asunto del distrito.

III. **<u>Uso Prohibido</u>**

A. Los empleados del distrito no deben usar la red para acceder a material obsceno, incluida la pornografía, o cualquier otro material que sea perjudicial para el propósito educativo y la misión del distrito o que sea incompatible con un entorno de trabajo profesional. Si se accede inadvertidamente a dicho material, un empleado del distrito debe notificar a su supervisor tan pronto como sea razonablemente posible.
B. Violar cualquier ley estatal o federal u ordenanza municipal, acceder o transmitir pornografía de cualquier tipo, representaciones obscenas, materiales dañinos, materiales que animen a otros a violar la ley, información confidencial omateriales protegidos por derechos de autor.
C. Vender o comprar artículos o sustancias ilegales.
D. Causar daño a otros o daño a su propiedad, como:
    1. Usar lenguaje profano, abusivo o descortés; amenazar, acosar, intimidar o hacer declaraciones dañinas o falsas sobre otros;
    2. Acceder, transmitir o descargar materiales ofensivos, acosadores o denigrantes;
    3. Dañar equipos informáticos, archivos, datos o la red de cualquier forma, incluido el acceso, la transmisión o la descarga intencionales de virus informáticos u otros archivos o programas dañinos; o interrumpir el rendimiento de cualquier sistema informático; causar daño físico a un recurso tecnológico; o
    4. Usar cualquier dispositivo para buscar "piratería", interna o externa al Distrito, o intentar acceder o almacenar información protegida por las leyes de privacidad.
E. Participar en usos que pongan en peligro el acceso o conduzcan al acceso no autorizado a las cuentas de otros u otras redes informáticas, como:
    1. Intentar obtener acceso no autorizado a la red o a cualquier otro sistema informático a través de la red o ir más allá de su acceso autorizado.

2. Usar la(s) contraseña(s) o identificador(es) de la cuenta de otra persona;
3. Interferir con la capacidad de otros usuarios para acceder a su(s) cuenta(s);
4. Revelar la contraseña de alguien o permitir que una persona use la(s) cuenta(s) de otro usuario;
5. Proporcionar la información de su cuenta, incluidas las contraseñas, a otros, o hacer que su cuenta sea fácilmente accesible. Compartir sus credenciales de usuario con el departamento de TI para solucionar problemas es una excepción;
6. Borrar, copiar, modificar o falsificar nombres, correos electrónicos, archivos o datos de otros usuarios; ocultar la propia identidad, hacerse pasar por otros usuarios o enviar correos electrónicos; o
7. Publicar o distribuir información personal sobre otro personal del Distrito en el sitio web del Distrito o Internet público sin el permiso del empleado o hacer referencia a información confidencial del estudiante en el sitio web del Distrito o Internet público.

F. Usar la red para:
    1. Beneficio financiero personal;
    2. Publicidad personal, promoción o ganancia financiera;
    3. Llevar a cabo actividades comerciales con fines de lucro y/o participar en actividades de relaciones públicas o de recaudación de fondos no relacionadas con el gobierno, como solicitudes con fines religiosos, cabildeo con fines políticos personales; o
    4. Usar software o hardware diseñado para interferir o eludir los mecanismos de seguridad.
    5. Usar la red de cualquier manera que viole cualquier regla o política del Distrito o de la escuela, incluidas, entre otras, cualquier otra regla o política.
G. Google Apps for Education - PTS utiliza Google Apps for Education para la colaboración en línea con el personal y los estudiantes. Los usuarios aceptan no utilizar los servicios de Google Apps for Education:
    1. para generar o facilitar correo electrónico comercial masivo no solicitado;
    2. 2. violar o alentar la violación de los derechos legales de otros;
    3. para cualquier propósito ilegal, invasivo, infractor, difamatorio o fraudulento;
    4. para distribuir intencionalmente virus, trabajos, caballos de Troya, archivos corruptos, engaños u otros elementos de naturaleza destructiva;
    5. para interferir con el uso de los Servicios, o el equipo utilizado para proporcionar los Servicios, por parte de clientes, revendedores autorizados u otros usuarios autorizados;
    6. para alterar, deshabilitar, interferir o eludir cualquier aspecto de los Servicios;
    7. para probar o aplicar ingeniería inversa a los Servicios para encontrar limitaciones, vulnerabilidades o evadir las capacidades de filtrado.
H. Ningún usuario establecerá una red de igual a igual o inalámbrica ad-hoc utilizando su dispositivo personal o cualquier otro dispositivo inalámbrico mientras se encuentre en la propiedad del distrito. Esto incluye, entre otros, el uso de un dispositivo electrónico de propiedad privada, como un punto de acceso inalámbrico o por cable.

I. El uso de una cuenta del Distrito es un privilegio, no un derecho. El mal uso podría resultar en la restricción o cancelación de la cuenta. El mal uso también puede dar lugar a otras acciones disciplinarias y/o legales tanto para los estudiantes como para los empleados, incluida la suspensión, expulsión, despido del empleo del Distrito o, en el caso de un estudiante de la escuela, o enjuiciamiento penal por parte de las autoridades gubernamentales. El Distrito intentará adaptar cualquier acción disciplinaria para satisfacer las inquietudes específicas relacionadas con cada infracción. En su caso, las sanciones a los empleados se harán de conformidad con el convenio laboral correspondiente.

IV. **Seguridad de Internet**

1. De acuerdo con la Ley de Protección de Niños en Internet (CIPA), el Distrito utilizará medidas de protección tecnológica en la red para bloquear o filtrar, en la medida de lo posible, el acceso a representaciones visuales que sean obscenas, pornográficas y/o dañinas para los menores.
2. El uso de la red del Distrito constituye consentimiento para ser monitoreado. Los usuarios no deben tener ninguna expectativa de privacidad con respecto a su uso de la propiedad del Distrito, la red y/o el acceso a Internet, los archivos y otros sistemas del Distrito, incluido el correo electrónico. Las tecnologías de monitoreo pueden usarse para identificar y mitigar problemas con el acceso a materiales inapropiados .
3. La intención de Phoenix-Talent Schools es educar a nuestros estudiantes para que sean buenos ciudadanos cibernéticos. Con aportes de administradores de edificios, maestros, líderes educativos y padres, Tecnología de la Información proporcionará recursos y planes de estudio sobre temas como:
    a. Seguridad de los menores cuando usan tecnología como sitios web de redes sociales, correo electrónico, videojuegos, salas de chat, mensajería y otras formas de comunicaciones electrónicas directas;
    b. Comportamientos en línea respetuosos y apropiados;
    c. Concienciación y respuesta al ciberacoso;
    d. Concienciación sobre ciberética, incluido el plagio, el engaño y la alfabetización informacional.