ECSD Acceptable Use Agreement

Acceptable Use Agreement

Purpose

The purpose of the Elko County School District Acceptable Use Agreement is to establish acceptable practices regarding the use of ECSD Technology Resources.

Audience

The ECSD Acceptable Use Agreement applies to any individual, entity, or process that interacts with any ECSD Technology Resources.

Acceptable Use

- Staff and Students are responsible for complying with ECSD policies when using ECSD Technology Resources . If requirements or responsibilities are unclear, please seek assistance from the ECSD IT Department.
- Staff must promptly report the theft, loss, or unauthorized disclosure of ECSD **confidential** or **internal information** to the ECSD IT Department.
- Staff or Students shall not purposely engage in any activity that may
    - harass, threaten, or abuse others;
    - degrade the performance of ECSD **Technology Resources**;
    - deprive authorized ECSD Staff or Students access to an ECSD **Technology Resource;**
    - utilize additional resources beyond those allocated; or
    - circumvent ECSD computer security measures or content filters.
- Staff and Students shall not download, install, or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, ECSD Staff and Students should not run password cracking programs, packet sniffers, port scanners, or any other non-approved programs on any ECSD **Technology Resource**.
- All inventions, intellectual property, and proprietary information, including reports, drawings, blue prints, software codes, computer programs, data, writings, and technical information, developed on ECSD time and/or using ECSD **Technology Resources** are the property of ECSD.
- Use of encryption should be managed in a manner that allows designated ECSD Staff and Students to promptly access all authorized data.
- ECSD **Technology Resources** are provided to facilitate District business and should not be used for personal financial gain.
- Staff and Students are expected to cooperate with incident investigations, including any district, local, state, or federal investigations.
- Staff and Students are expected to respect and comply with all legal protections provided by patents, copyrights, trademarks, and intellectual property rights for all software and/or materials viewed, used, or obtained using ECSD **Technology Resources**.
- Staff and Students shall not intentionally access, create, store or transmit materials which ECSD may deem to be offensive, indecent, or obscene.

Access Management

- Access to information is based on a "need to know" basis with proper authorization.

- Staff and Students are permitted to use only those network and host addresses issued to them by ECSD IT and should not attempt to access any data or programs contained on ECSD systems for which they do not have authorization or explicit consent.
- All remote access connections made to internal ECSD networks and/or environments must be made through approved, and ECSD-provided, virtual private networks (VPNs).
- Staff shall not divulge any access information to anyone not specifically authorized to receive such information.
- Staff and Students must not share their ECSD authentication information, including:
    - Account passwords,
    - Personal Identification Numbers (PINs),
    - Security Tokens (i.e. Smartcard),
    - Access cards and/or keys,
    - Digital certificates, and
    - Similar information or devices used for identification and authentication purposes.
- Lost or stolen access cards, security tokens, and/or keys must be reported to administration as soon as practical.
- A service charge may be assessed for access cards, security tokens, and/or keys that are lost, stolen, or are not returned.

Authentication/Passwords

- All Staff and Students are required to maintain the confidentiality of personal authentication information.
- Any group/shared authentication information must be maintained solely among the authorized members of the group.
- All passwords, including initial and/or temporary passwords, must be constructed and implemented according to the following ECSD rules:
    - Must meet password complexity requirements.
    - Must not be easily tied to the account owner by using information like: user name, social security number, nickname, relative's names, birth date, etc.
    - Should not include common words, such as dictionary words or acronyms.
    - Should not be the same passwords as used for non-business purposes.
- Unique passwords should be used for each system, whenever possible.
- User account passwords must not be divulged to anyone. ECSD Staff, Students and contractors should never ask for user account passwords.
- Security tokens (i.e. Smartcard), if issued, must be returned on demand or upon termination of the relationship with ECSD.
- If the security of a password is in doubt, the password should be changed immediately.
- Staff and Students should not circumvent password entry with application remembering, embedded scripts, or hard coded passwords in client software.

Data Security

- Only authorized **cloud computing applications** may be used for sharing, storing, and transferring **confidential** or **internal information**.
- Information must be appropriately shared, handled, transferred, saved, and destroyed based on the information sensitivity.

- All electronic media containing confidential information must be securely disposed of. Please contact IT for guidance or assistance.

Email and Electronic Communication

- Electronic communications shall not misrepresent the originator or ECSD.
- Staff and Students are responsible for the accounts assigned to them and for the actions taken with their accounts.
- Account credentials must not be shared without prior authorization from ECSD IT.
- Employees shall not use personal email accounts to send or receive ECSD **confidential information**.
- Personal use of ECSD email accounts is discouraged.
- Any personal use of ECSD provided email shall not:
    - Involve solicitation.
    - Have the potential to harm the reputation of ECSD.
    - Forward chain emails.
    - Contain or promote anti-social or unethical behavior.
    - Violate local, state, federal, or international laws or regulations.
    - Result in unauthorized disclosure of ECSD **confidential information**.
- Staff and Students shall only send **confidential information** using secure electronic messaging solutions.
- Staff and Students should use caution when responding to, clicking on links within, or opening attachments included in electronic communications.
- Staff and Students should use discretion in disclosing **confidential** or **internal information** in “Out of Office” or other automated responses, such as employment data, internal telephone numbers, location information, or other sensitive data.

Hardware and Software

- All hardware must be formally approved by IT Management before being connected to ECSD networks.
- Software installed on ECSD equipment must be approved by IT Management and installed by ECSD IT.
- All ECSD assets taken off-site must be physically secured at all times.
- Employees shall not allow family members or other non-employees to access ECSD **Technology Resources**.

- Any person who has ECSD devices checked out to them, are responsible for that device. Failure to return the device, in working condition, when requested will result in fees that are outlined in the ECSD Chromebook Manual.

Internet

- The Internet must not be used to communicate ECSD **confidential** or **internal information**, unless the confidentiality and integrity of the information is ensured and the identity of the recipient(s) is established.

- Use of the Internet with ECSD networking or computing resources must only be for educational, or business-related activities. Unapproved activities include, but are not limited to:
    - Recreational games,
    - Streaming media,
    - Personal social media,
    - Accessing or distributing pornographic or sexually explicit and/or oriented materials, and
    - Attempting or making unauthorized entry into any network or computer accessible from the Internet.
    - Bypassing content filters
- Access to the Internet from outside the ECSD network using an ECSD owned computer must adhere to all of the same policies and procedures that apply to use from within ECSD facilities.

Mobile Devices and Bring Your Own Device (BYOD)

- ECSD does not allow **personally-owned mobile devices** to connect to the ECSD internal network.
- Mobile devices that access ECSD email must have a PIN or other authentication mechanism enabled.
- ECSD **confidential information** shall not be stored on any personally-owned **mobile device**.
- Theft or loss of any **mobile device** that has been used to create, store, or access **confidential** or **internal information** must be reported to the ECSD IT Dept immediately.

- All Staff and Students are expected to use **mobile devices** in an ethical manner.
- Jail-broken or rooted devices shall not be used to connect to ECSD **Technology Resources**.
- ECSD IT Management may choose to execute "remote wipe" procedures for **mobile devices** without warning.
- In the event there is a suspected incident or breach associated with a **mobile device**, it may be necessary to remove the device from the Staff or Student's possession as part of a formal investigation.
- All mobile device usage in relation to ECSD **Technology Resources** may be monitored, at the discretion of ECSD IT Management.
- ECSD IT support for personally-owned **mobile devices** is limited to assistance in complying with this Agreement. ECSD IT support may not assist in troubleshooting device usability issues.
- Use of **personally-owned** devices must be in compliance with all other ECSD policies.
- ECSD reserves the right to revoke **personally-owned mobile device** use privileges in the event that Staff or Students do not abide by the requirements set forth in this Agreement.

Privacy

- Information created, sent, received, or stored on ECSD **Technology Resources** is not private and may be accessed by ECSD IT employees at any time, under the direction of ECSD executive management and/or Human Resources, without the knowledge or consent of the user or resource owner.
- ECSD may log, review, and otherwise utilize any information stored on or passing through its **Technology Resources**.

- Systems Administrators, ECSD IT, and other authorized ECSD Staff may have privileges that extend beyond those granted to standard Employees. Employees with extended privileges shall not access files and/or other information that is not specifically required to carry out an employment related task.

Social Media

- Communications made through social media shall be made in compliance with this Agreement and all applicable ECSD policies.
- Staff and Students are personally responsible for the content they publish online. No such content is adopted or endorsed by the District unless specifically stated as such.
- Creating any public social media account intended to represent ECSD, including accounts that could reasonably be assumed to be an official ECSD account, is prohibited without the permission of the Superintendent or designee.
- When discussing ECSD or ECSD-related matters, you should:
    - Identify yourself by name,
    - Identify yourself as an ECSD representative, and
    - Make it clear that you are speaking for yourself and not on behalf of ECSD, unless you have received explicit approval to do so.
- Staff and Students shall not misrepresent their role at ECSD through an email signature or otherwise.
- When publishing ECSD-relevant content online in a personal capacity, a disclaimer should accompany the content. An example disclaimer could be: “The opinions and content are my own and do not necessarily represent ECSD’s position or opinion.”
- Content posted online must not violate any applicable laws (i.e. copyright, fair use, financial disclosure, or privacy laws) or be defamatory.
- Discrimination (including age, sex, race, color, creed, religion, ethnicity, sexual orientation, gender, gender expression, national origin, citizenship, disability, marital status or any other legally recognized protected basis under federal, state, or local laws, regulations, or ordinances) in published content that is affiliated with ECSD is illegal and will not be tolerated.
- Confidential information, internal communications, and non-public financial, personal or operational information may not be published online in any form.
-

Incidental Use

- As a convenience to ECSD Staff and Students, incidental use of **Technology Resources** is permitted with the following restrictions:
    - Incidental personal use of electronic communications, Internet access, fax machines, printers, copiers, etc., is restricted to ECSD approved Staff and Students; it does not extend to friends, family members or other acquaintances.
    - Incidental use must not result in any direct costs to ECSD.
    - Incidental use should not interfere with the normal performance of an employee’s work duties.

    - No files or documents may be sent or received that may cause legal action against, or embarrassment to, ECSD or its staff and students.
- Storage of personal email messages, voice messages, files and documents within ECSD **Technology Resources** must be nominal.
- All information located on ECSD **Technology Resources** is owned by ECSD, may be subject to **Nevada Public Records Act** records requests, and may be accessed in accordance with this Agreement.

Enforcement

Students found to have violated this Agreement may be subject to revocation of technology privileges, disciplinary action, and related civil or criminal penalties.

Staff and Students found to have violated this agreement may be subject to disciplinary action, up to and including termination of employment or expulsion, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this Agreement may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.