Environmental Charter Schools

Computer Usage Policy

Environmental Charter Schools ("ECS") provides the academic community at its sites with computer systems to support instruction and research. Access to these computer systems is a privilege offered to ECS faculty, staff, administration, students, certain authorized individuals performing work for institutes and affiliates of ECS, and other individuals affiliated with ECS (collectively, "Users"). ECS may revoke this privilege and/or take other disciplinary action against any individual who fails to comply with the ECS Computer Policy set forth herein and as it may be amended from time to time (the "Computer Usage Policy").

Users must read carefully the Computer Usage Policy and be certain that they understand it before using a computer system provided by ECS. Please contact the Chief Education Officer ("CEO") or designee with any questions. Your use of Resources (defined below) signifies that you have read the Computer Usage Policy and agree to follow it.

Violations of the Computer Usage Policy may result in:

(i) Suspension or revocation of your access privileged,
(ii) Disciplinary action as a described in the Student Code of Conduct and Disciplinary Procedures,
(iii) Disciplinary procedures of ECS under the relevant policies for faculty, staff, administration, and students, and/or
(iv) Civil or criminal prosecution under federal and/or state law. Penalties under such laws include fines, orders of restitution, and imprisonment.

ECS Computer Usage Policy

1. Users may not tamper with ECS computers, computer systems, networks, facilities, equipment, software, files, documentation, accounts, or information associated with any of them (collectively, "Resources"). This Computer Usage Policy regulates the direct and indirect use of Resources both on-campus and off-campus.
2. All potential Users may use Resources so long as they qualify and comply with the Computer Usage Policy. Non-Users are not permitted access to Resources.
3. Unauthorized attempts to gain access to Resources or any account not belonging to you, as a User, on any ECS system or any other system is not permitted. Assisting others in gaining unauthorized access to such Resources or accounts, including your own account, is not permitted.

4. Users may not access or copy directories, programs, files, data, or documents (including music and video) which do not belong to you unless you have permission from the account holder, copyright holder or owner to do so and permission is received in writing signed by the CEO or designee.
5. Except with prior explicit written permission from the CEO or designee, Resources must not be used for commercial purposes or monetary gain.
6. ECS, the damaged party or the appropriate legal authority reserves the right to hold you financially, civilly or criminally liable if, through negligence or deliberate action, Resources are compromised in any way by you or someone using Resources.
7. Downloading music, video, movie or other copyrighted material from public networks or peer computers is strictly forbidden unless it is specifically approved in writing and signed by the CEO or designee.
8. In the event you are assigned a password for access to Resources, you are prohibited from disclosing your password to any individuals, except to the CEO or designee. Users must safeguard your account and its contents, and will be responsible for any misuse. Users may not search for, access, copy, or use passwords belonging to other people.
9. Use of software applications/programs or internet sites that penetrate firewalls or attempt to bypass secured files (such as those that are password protected) or crack or hack user accounts is strictly forbidden unless approved and/or overseen by CEO or designee. In such case, permission must be in writing and signed by CEO.
10. An account owner (User/Person) may not lend or transfer his/her account(s) to another User/Person.
11. Each account owner is responsible for all computing activities involving that account, and will be held liable for any misuse of that account.
12. Users may not use Resources to misrepresent himself/herself as another individual (“spoofing”). If you are a victim of such misrepresentation, you must immediately upon discovery of the incident report the incident to the CEO or designee.
13. No User may use, or attempt use, any computer accounts other than his/her own assigned account. The negligence or naiveté of another User/Person in revealing an account name and password does not confer authorization to use the account.
14. Users must have written permission from the CEO or designee to remove or copy any Resource owned or licensed by ECS. Users may not copy any software or document unless you are licensed by the software licensor to do so, or unless the software or document is from ECS public domain library. Users may not

remove Resources from their designated places without permission of the CEO or designee.

15. Users may not use Resources to send, forward, or otherwise disseminate nuisance messages. Nuisance messages include, without limitation, messages sent to a recipient who has previously notified you that messages of a particular type from you will constitute a nuisance.
16. Users may not use Resources to access obscene, graphic, pornographic or offensive material.
17. Users may not use Resources in such a way as to create or constitute, in the sole determination of the CEO or designee, an unacceptable burden on Resources. Nonexclusive examples of such acceptable burdens include mail bombing, creating an excessive number of sessions, registering custom (non-ECS) domain names, and creating unnecessarily large files.
18. Users must comply with all applicable CEO or designee technical policies. If you have questions regarding such policies, please contact the CEO or designee.
19. Users may not use Resources in connection with activities prohibited by any applicable ECS policy or by any applicable laws, ordinances, rules, regulations, or orders of any public authority having jurisdiction including, without limitation, those concerning: trademark, copyright, and other intellectual property, unauthorized use of a person's image, civil rights, commerce, computer usage, conspiracy, telecommunications, defamation, forgery, obscenity, and privacy (collectively, "Laws").
20. E-mail and other computer files (collectively, "Files") can never be considered fully private, particularly in light of (i) the open nature of the Internet and related technology and (ii) the ease with which Files may be accessed, copied, and distributed. Users are advised to avoid sending messages by e-mail and storing information in computer files that are of a confidential or extremely personal nature (including, but not limited to credit card or social security numbers).
21. Users must comply with the ECS Software Policy and all other applicable policies related to Resources.
22. Any exception to the access policies stated in this Policy must be approved in writing by the CEO or designee.
23. As ECS understands the sensitive nature of the information stored in its databases or on its network ("Information"), ECS has a written confidentiality policy providing protection of such Information. Every effort is used to protect the Information and ECS does not allow access or use of the Information except in cases where it is specifically required by law. Any attempt by a User to gain access to the Information or to change, manipulate, or otherwise damage its integrity will be prosecuted to the full extent allows by law. Additionally, each User by using Resources explicitly understands that the Information is

confidential and as such disseminating it outside ECS for any reason is expressly prohibited.

_____ _____

Employee Signature Date

_____

Print Name