

Appendix B - Unacceptable Uses of IT Resources

1. Employees will not use state-provided IT resources for inappropriate purposes or in support of such activities. This includes, but is not limited to the following:
 - a. any use which violates local, State, or Federal laws;
 - b. any use for commercial purposes, product advertisements, or "for-profit" personal activity;
 - c. any use for viewing, transmitting, receiving, saving, or printing sexually explicit material;
 - d. any use for religious or political lobbying;
 - e. any use in relation to copyright infringement;
 - f. any use of the Internet other than for official DHHR business;
 - g. any use in relation to downloading or installing any software or inappropriate files (ex:MP3 files);
 - h. any use in relation to participating in chain letters or chat programs;
 - i. any use for promoting discrimination on the basis of race, gender, national origin, age, marital status, sexual orientation, religion, or disability;
 - j. any use for promoting the use of weapons or devices associated with terrorist activities;
 - k. any use for dispersing data to customers or clients without authorization; or
 - l. any use in relation to gambling
2. Employees will not waste IT resources by intentionally doing one or more of the following:
 - a. placing a program in an endless loop;
 - b. printing unnecessary amounts of paper;
 - c. disrupting the use or performance of state-provided IT resources or any other computer system or network; or
 - d. storing unauthorized information or software on state-provided IT resources.
3. Employees will not knowingly or inadvertently commit security violations. This includes doing one or more of the following:
 - a. accessing records within or outside the state's computer and communications facilities for which the employee is not authorized;
 - b. copying, disclosing, transferring, examining, re-naming, or changing information or programs belonging to another user unless given express permission to do so by the user responsible for the information or programs;
 - c. violating the privacy of individual users by reading e-mail or private communications unless the employee is specifically authorized to maintain and support the system; or
 - d. misrepresenting oneself or the State.
4. Employees will not knowingly or inadvertently spread computer viruses. To reduce this threat, employees must not import files from unknown or questionable sources.