

River Valley Child Development Services

Information Technology (IT) Procedure

Effective: December 1, 2016

Initial training on the IT policy procedure will be provided at program orientation and as new technology is introduced. The Program Director will provide annual review of this procedure. All employees must complete an Information Technology Responsibility and Use Agreement. For assistance or clarification please see your supervisor or Program Director.

Section I- Information Security/Protection of Confidentiality

- Access only files, data and protected records that are your own, that are publicly available, or to which you have been given authorized access.
- Utilize IT resources efficiently and productively. Refrain from monopolizing systems, overloading networks with excessive data, bandwidth, disk space, or other IT resources.
- Prevent unauthorized access- all devices should be set to use auto lock.
- Make sure virus protection is current and performed regularly.
- Report to your supervisor if you:
 - Receive or obtain information to which you are not entitled. (Note: also notify the owner or sender of the information.)
 - Become aware of breaches of security.

Section II-Physical Security

- The Information Technology Responsibility and Use Agreement must be completed by each user of IT resources (stationary and portable). The original copy is maintained by the Program Director or supervisor.
- Provide proper care and maintenance of all IT resources assigned to you.
- Take reasonable care not to abuse or damage IT resources and use precaution with food and drink around IT resources.
- Portability increases the risk of damage, loss, or theft from employee's home or vehicle, or during use in public areas. IT resources should always be transported in protective cases and should never be left unattended. If left in the employee's vehicle, it must be out of view and vehicle must be locked.
- Individuals/Employees found negligent for lost, stolen or damaged IT resources are responsible to pay the full costs of the replacement. Normal wear and tear will not be considered negligent.
- Individuals agree to pay via personal check, money order, or can have charges deducted from their paycheck, either as a one-time deduction or spread over multiple paychecks, as determined by employee and Program Director. The payments must begin within 30 days of arrangement.

Section III- Unacceptable Use of IT Resources

Inappropriate use of IT resources poses a risk of disruption of IT resources and is prohibited. The first and foremost rule for using these technologies is: **Don't say, do, write, invite or acquire anything that you wouldn't be proud to have everyone in the world learn about if the electronic records are laid bare.**

When using IT resources there must be:

- No use in support of illegal activities.
- No use for personal profit activity.
- No sexually explicit use.
- No religious or political lobbying.
- No copyright infringement.
- No distribution of offensive or harassing statements.
- No downloading of internet programs, program updates, or inappropriate customizing of a computer beyond the needs of the employee's duties without permission from the supervisor.
- No distributing or forwarding "junk mail".
- No excessive storing or printing of personal information not authorized by the agency.

Section IV- Disposition of IT

Each program is responsible to create and follow a disposition procedure using the guidelines of their grant and/or agency requirements.

Section V- Policy Enforcements & Disciplinary Actions

The Program Directors or designees will monitor and provide ongoing enforcement of the IT policy. In order to monitor this, reports will be created for review.

The Program Director is the primary authority to investigate any suspected instances of misconduct involving IT resources. Employees with access to any IT resource may be denied or revoked access based upon the investigation. Violations, including the inability to fulfill the requirements of one's job due to the revocation of IT resource privileges, could result in discipline according to the current RVCDS disciplinary policy.