Procedures for Recording, Storage and Use of Data Collected at the Child Development Center for Learning and Research, as specified by the VT Institutional Review Board

1. Any electronic format which includes a child's identifying information for research purposes (name, birthdate, facial image, etc.) must be either:

a) Recorded, stored and used only on a computer that does not have internet access, and cannot be copied to jumpdrive or other type of data storage device that could be connected to the internet;
b) Encrypted. If the latter, can be transferred across the Internet, with password to decrypt given orally or in other fashion not linked with the relevant datafile, to the receiver.

2. Anonymous data – use of ID codes only, for example – can be stored and communicated via internet-access computers.

3. Observational records, written or word-processed narratives that are not encrypted must protect CDCLR children and staff identities by referring to them by a code. This code must not be able to be used to personally identify a participant (for example, use of birthdate, address or other numeric identifier linked to the participant.)

Ideally all observational records and narratives will be so identified. Keys to the codes must be kept in a secure location as approved by the VT IRB, and not on any electronic device that is not secure (i.e., that has internet-access or that is available to users other than those supervised by the Principal Investigator(s) of the approved research project).

In cases where it is not practicable (for instance, when observers don't know the children and identify them by name and picture), those records must be stored at CDCLR. Once the information is ready to transfer to the external investigator, he/she or a qualified representative (i.e, a trained student) will meet with the CDCLR Research Director to assign code numbers to the research participants. Once data is completely anonymous, a researcher can take remove the data from CDCLR. The key codes will stay with the CDCLR Research Director in locked files and will be accessible to the researcher upon request, with appropriate safeguards regarding information transfer in place. (If external researcher has encryption capability, follow 1b.)

4. Audio, video and digital recordings:

- All recordings must be labeled by a code. Key for code follows above procedures.
- Recordings must be kept in a locked, secure facility.
- Recordings must be erased or otherwise destroyed at parent's or participants' request.