Guidelines for Sensitive Data Security Plan for the Use of Child Development Project Data

The fundamental goal of the protections outlined in the Data Security Plan is to prevent persons who are not signatories to the Data Use Agreement or are not included in the Supplemental Agreement with Research Staff from gaining access to the data. When these agreements are executed, all members of the research team are obligated to follow all aspects of the Sensitive Data Security Plan.

General Information Required:

1. Title of Research Project
2. The names, titles, and responsibilities of all the investigators(s) and research staff (students, research assistants, and programmers) who will have access to the data. Any changes in personnel require the submission of updated information.

3. A detailed description of the computer system where the data will be stored and analyzed. This description should include the following:

    - All locations where copies of the data and paper files will be kept.

    - The computing platform, number of computers on which data will be stored or analyzed, whether personal computers will be stand-alone or networked, the physical environment in which computers are kept, and who has physical access to the equipment.

    - The devices on which data will be stored, how the computer system handles backups, and how long system backup copies of the data are kept.

    - Information on the security of the backup copies of the data made by the research team, including the original data sent by Child Development Project and temporary analysis files. Temporary files must be deleted at the end of each year and re-created, if necessary, to complete the research.

    - The security system that would prevent unauthorized access to the data, and whether this system is used by other projects.

4. The time frame for analysis of the data, including the end date of the project. This date should not exceed three years from the execution of the data use agreement. Should the research project require additional time, a request for continuation should be submitted three months prior to the specified end date. Unless prior arrangements are made with the Child Development Project Data Center, all electronic and paper data must be destroyed on the end date.

Specific Guidelines:

1. The use of stand-alone personal computers with data stored on the hard drive is strongly discouraged. It is preferred that the data be stored on a secure network. If, however, a network is not available, then the personal computer must meet the current Child Development Project policy. That is, the computer must be located in a locked office, with access restricted to project personnel only. Further, the computer must be secured to a stationary object (such as a desk) using an Anchor Pad® (or similar device) and the case itself must be secured so that the hard drive could not be removed. Use of the computer is restricted to project personnel only, with password-protected access to the computer. The use of personal firewalls is strongly recommended.

2. For sites using local area networks, security of the file server must follow Child Development Project policies. That is, the file server needs to be located in a room with access restricted to network administrators. The unit itself must be secured to a stationary object (such as a desk) using an Anchor Pad® (or similar device) and the case itself must be secured so that the hard drive(s) could not be removed (this includes securing access to "hot-swappable" drives). It is strongly recommended that the file server be up-to-date and maintain constant monitoring and application of available security patches. All authorized users must have a user name and a "strong" password to access the file server (strong passwords cannot use any word found in a standard dictionary, names of relatives, and must be made up of upper and lower case letters and numbers). If the data will be stored on a mainframe computer, then it is strongly recommended that the researcher contact the computer security officer to ensure that the data remain secure.

3. No data or analysis output derived from the data can be transmitted via e-mail, e-mail attachments, or FTP.

4. The original copy of the data supplied by Child Development Project is the only backup copy allowed, and must be kept in the Duke Box folder in which it was originally provided.

5. Removable storage devices holding temporary data files must be kept in a locked compartment when not in use.

6. Printouts derived from data analysis must be stored in a locked compartment when not being used. Printed information that is no longer needed should be shredded before disposal. Printouts of data from Child Development Project are not to be distributed to anyone outside of the research team.